Safe harbour agreement implementation stuydy : draft submited March 1, 2004

Dhont, Jan; Pérez Asinari, María Veroníca; BYGRAVE, Lee; REIDENBERG, Joel; Poullet, Yves

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

Safe Harbour Agreement Implementation Study

prepared by

Dr. Yves Poullet, Jan Dhont and María Verónica Pérez Asinari (CRID)

with the assistance of

Dr. Lee Bygrave and Dr. Joel Reidenberg

at the request of the
European Commission, Internal Market DG

Draft submitted March 1, 2004

Index

I. Introduction

The SH "SH")[1] Agreement issued by the United States Department of Commerce (DoC) for the transfer of personal data from the European Union (EU) to the United States (US) is recognized by the European Commission as providing "adequate" protection under the terms of Directive 95/46/EC. The SH documents create a voluntary mechanism that enables US organizations to qualify for data transfers from the EU. In particular, SH defines a set of privacy principles and frequently asked questions (FAQs), allowing US organizations to commit that their information practices will conform to the defined principles, and requires the availability of independent recourse mechanisms for enforcement. The commitment by organizations processing European data must be made to the DoC through a certification that publicly identifies the organization's adherence to the principles. This commitment being made, companies are bound by the SH.

Pursuant to Article 4 (1) of the Commission Decision, the implementation of the Decision is subject to an evaluation three years after its notification to the Member States.

At the request of the European Commission, this report researches and reports on the implementation of SH. The specific objectives and methodology for the research are described in Section II. Section III describes the results of the study, and include (i) a brief theoretical overview of the SH regime; (ii) a factual analysis of the SH certification pages published on the DoC SH website; (iii) a deep-level analysis of the implementation of the SH principles; and (iv) a contextual analysis of the SH principles. The report concludes in Section IV with an evaluation of the current implementation of the SH in light of findings.

[1] The SH entails the principles and the FAQs as set forth in the Commission Decision of 26 July 2000.

II. Objectives and Methodology

A. Objectives

The task assigned by the European Commission consists of an analysis *of the implementation of the SH Agreement.* More precisely this study seeks to identify trends in the compliance of registered organizations with the terms of the SH Agreement and to determine the extent to which registered organizations generally:

1. rely on a privacy policy which covers all SH principles and which is publicly displayed so as to trigger Section 5 of the US Federal Trade Commission Act;
2. fulfil the requirements laid down in FAQ 6 (as regards their Self-Certification), FAQ 7 (as regards their Verification procedures) and FAQs 5 and/or 11 (with regard to their Independent Dispute Resolution System and Enforcement);
3. operate within the jurisdiction of the Federal Trade Commission (FTC) or Department of Transportation (DOT);
4. signal in their privacy policy whether and if so the extent to which prevailing laws in the US prevent them from applying the SHA.[2]

The study also seeks to report whether the independent dispute resolution mechanisms chosen by registered organizations generally appear to satisfy the requirements of FAQ 11 and, in particular, if seal organizations or privacy programs offering dispute resolution respect FAQ 11.[3] Additionally, this study will examine some of the implementation experiences of different interested parties, specifically US and EU public and private bodies. The study focuses on the *implementation* of the SHA and does not review the SHA itself.

Finally, the collateral impact of certain regulatory regimes on the SH principles are analysed: (1) impact of other transborder data flow regimes; and (2) the impact of new US federal legislation on the application of the SHA.

B. Methodology

1. Theoretical Overview

1.1. Scope of application

[2] These tasks track the Independent Consultant Study, Interim Report on the Implementation of SH (September 21, 2001)
[3] Id.

This part provides a brief theoretical overview of the scope of application of the SH regime (*ratione materiae*, *ratione personae*, *ratione loci*). It provides the theoretical background against which the factual, deep-level and contextual analysis is conducted. It does not aim to exhaustively explain the principles, but to help orientating the reader who is not acquainted with the SH framework.

1.2. Involved Actors

Part 1.2 focuses on the role played by each actor involved in the SH system, (i.e. public bodies in Europe and the United States, companies, dispute resolution bodies, intermediary associations, etc.). It identifies these actor's functions within the SH framework. The aim of this point is to indicate the capacities and limits of each actor in order to have a better understanding of their responsibilities.

2. Certification Page Analysis

The description of the scope is complemented by an analysis of factual data extracted from the certifications available on the SH list published on the DoC website. This survey concerns all companies that have self-certified as of November 3, 2003. It aims at having an overview of the SH self-certification state-of-the-art. The analysis exhaustively reviews the following elements as shown on the DoC certification form:

- The industry sector in which the certifying entity is active;
- Data typology;[4]
- On-line, off-line, manually processed data processing, and processing of human resources data;
- Accuracy of privacy policy location;
- The type of verification, i.e. in-house, third party or both;
- Whether entities fall under the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DoT), or none of them;
- Whether entities adhere to a privacy program;
- Type of dispute resolution mechanism to which entities are adhering;
- Whether entities have declared to co-operate with the European DPAs; and
- The privacy policy's certification status.

[4] Data types can be classified roughly, from the declaration made in the item "Personal Information Received from the EU", as: (1) commercial data; (2) human resources data; (3) research data (market and others); (4) travel data; and (5) medical data.

3. In-depth implementation analysis of the SH Regime

3.1 Visible compliance/implementation

This part is based on a survey of publicly available privacy policies of US companies adhering to the SH, as referred to in the certification page. It aims at obtaining a better view of the practical implementation of the SH principles. The research for this part consisted of three components:

(a) Selection of Organizations and Collection of Documents

The study selected 10% of all organizations that have self-certified their adherence to SH as of November 3, 2003. A sample of 10% was chosen since a thorough analysis of all SH companies was feasible within the frame of this study. The companies that have been subject to this review have been determined randomly.

During the week of November 3, 2003, the self-certification statements and the publicly available privacy policies of each of the organizations were printed from theDoC's web site and the respective web sites of each of the organizations. For one company, the relevant policy could not immediately be located, and was discovered and printed on January 30, 2004. Other policies, those declared to be available at physical addresses or Intranets, were requested to the companies by e-mails.

The 41 selected organizations listed the following privacy programs and/or independent dispute settlement mechanisms in their certifications to the US Department of Commerce:

1. Truste;
2. Better Business Bureaus Online ("BBBOnline");
3. American Arbitration Association ("AAA");
4. Coalition Against Unsolicited Commercial E-mail ("Cauce");
5. the Council of American Survey Research Organizations ("CASRO");
6. Direct Marketing Association SH program ("DMAshp");
7. Direct Marketing Association (without specifying the DMA SH program); *and*
8. Online Privacy Aliance ("OPA").

The publicly available materials on the policies and dispute settlement mechanisms of each of these programs were printed from each of the respective program's web sites during January and February 2004.

(b) The Analytical Criteria

Companies: The SH Privacy Principles and the FAQs were distilled into a checklist of 66 criteria.[5] For a company to conform to the requirements of SH, each of these analytical criteria must be satisfied from the aggregate of statements, disclosures and commitments made in the organization's self-certification, corporate privacy policy and independent dispute settlement mechanism.

These elements were divided into three categories:

1. those addressing *eligibility of organizations* to qualify for the benefits of SH including procedural requirements;
2. those addressing the *substantive provisions* of fair information practices; and
3. those addressing *enforcement mechanisms and remedies.*

To the extent possible, the analytical criteria were defined as objective conformity or non-conformity indicators with the SH and FAQs. The criteria for each category are listed and described in Appendix I. The meaning of these criteria is subject to a short comment.

Privacy programs: In addition, for privacy programs and their independent dispute resolution mechanisms, the SH and FAQ 11 were distilled into a checklist of 35 criteria. For the privacy program or dispute resolution mechanism to conform to SH, these criteria must be found in the privacy program or dispute resolution body's rules.

These elements were divided into groups as follows:

A. incorporation of SH *notice* principles in privacy program rules;
B. incorporation of SH *choice* principles in privacy program rules;
C. incorporation of SH *onward transfer* principle in privacy program rules;
D. incorporation of SH *security and integrity* principles in privacy program rules;
E. incorporation of SH *access* principle in privacy program rules;
F. incorporation of SH *enforcement* principles in dispute resolution including FAQ 11.

The elements for each category are listed in Appendix II.

The study analyses the programs that were named by reviewed SH companies as "privacy programs."[6] Further, dispute resolution mechanisms/programs that are mentioned in the reviewed companies' DoC certification page and that do not constitute a "privacy program" are assessed with respect to the requirements set forth by FAQ no. 11.

(c) Scoring

---

[5] This part of the study tracks criteria used in the Independent Consultant Study, Interim Report on the Implementation of SH (September 21, 2001).

[6] See *infra*, point 2.8

The research examined the publicly available information from each organization to ascertain if each element of the analytical criteria was satisfied.[7] The publicly available information consisted of the self-certification statements of each organization as found on the DoC's web site, the privacy policies referenced in those certifications, any other privacy policy found at each organization's web site when the location of the privacy policy in the certification was inaccurate, any other relevant policies mentioned on the web site of each organization or cross-referenced by the organization's privacy policy, and any e-mail requested privacy policy when appropriate (see *supra*).

For privacy programs and independent dispute settlement mechanisms, the study examined each organization's self-certification statement when available and the rules of each privacy program and dispute settlement mechanism as found on each program's web site.

Since the SH presents an alternative to statutory protection in the US, the analytical criteria were interpreted narrowly. For example, SH requires that organizations disclose the public location of their privacy policies in the self-certification letter. If an organization provides only the URL location of the general web site of the organization or an erroneous specific URL for its privacy policy, it scored a negative score for "accurate location."

At the same time, the terms of each organization's publicly available information were generally construed liberally. For example, the SH requires that organizations use reasonable security measures to protect personal information. If an organization indicated that it encrypted data or merely stated that its information was secure, then the organization would be scored as satisfying this element.

Because the underlying goal of SH is to provide a clear, high level of protection in the absence of an adequate personal data protection regime, any ambiguities or contradictions in an organization's publicly available information resulted in an adverse score. When an organization did not represent the SH obligations that are considered mandatory, the organization was scored as not satisfying the analytical element. When an organization's publicly available information was contradictory, the organization was scored as "unclear". If the policy was not made publicly available it scored an "unknown," while a "not applicable" was scored for most US organizations that are data processors. Finally, US organizations which are data controllers scored a "not applicable" for certain criteria if no obligations exist as a consequence of the absence of certain data processing activities. In that case, the organization scored a "napp." For instance, if an organizations does not represent to process sensitive data, opt-in is not required. Consequently, such organizations scored a "napp" for providing opt-in.

3.2. Case-Study

[7] This part tracks partly the scoring used in the Independent Consultant Study, Interim Report on the Implementation of SH (September 21, 2001).

A specific case-study has been conducted with volunteering companies. Volunteering companies were asked to answer the question list set forth in Appendix III. The purpose was to gain a better view of companies' practices beyond what is established in a privacy policy and to better understand how the abstract principles are put into practice. 3 companies volunteered to answer the questions. So far, one company answered. The answers have not been inserted in the report for reasons of confidentiality and lack of meaning (representedness).

3.3. ADR/ODR

Special attention was paid to the enforcement mechanisms, and in particular to the requirements of FAQ 11. The analytical criteria[8] already include specific issues to be evaluated with respect to the mechanisms that have to be present in the companies' Privacy Policies. A questionnaire was sent to 7 dispute resolution organizations referred to the website of the DoC . The relevant page mentions the following: "While programs vary, organizations like BBBOnline, TRUSTe, AICPA WebTrust, the Direct Marketing Association, the Entertainment Software Rating Board, JAMS and the American Arbitration Association have developed programs that assist in compliance with the SH's enforcement principle and FAQ 11."[9]

The questionnaire gauges the experiences that such dispute resolution bodies have with the SH regime. The questionnaire is attached to this report in Appendix III. Only one organization has answered to the questionnaire.

3.4 Implementation Experiences of Different Actors

Finally the study assesses implementation experiences by different actors involved in the SH mechanism. The solicited parties were (a) lawyers that have experience with transborder data flows between Europe and the US (15 lawyers have been approached, of which 4 answered); (b) national data protection authorities; the FTC; the DoC; and

---

[8] Independent Consultant's Study, Interim Report on the Implementation of SH (September 21, 2001).

[9] See "Helpful Hints Prior to Self-Certifying to the Safe Harbor", DoC, available at: http://www.export.gov/safeharbor/helpful_hints.html , last visited 23/02/04. On "Safe Harbor Workbook", the DoC adds: "A third-party dispute resolution mechanism assures your customers that your organization is complying with its stated policies. While programs vary, organizations such as BBBOnLine, the Direct Marketing Association, the Privacy Council and the Entertainment Software Rating Board have indicated that they have developed privacy programs that allow companies to comply with the Safe Harbor privacy principle on enforcement. Other programs such as an outside arbitration and mediation service (e.g. JAMS or the American Arbitration Association) may also be used, so long as every complaint is heard in compliance with the enforcement principle and FAQ 11. ***(Note: Organizations self-certifying to the Safe Harbor are responsible for ensuring that they have chosen a dispute resolution provider that will satisfy the requirements of the framework. The Department of Commerce does not certify programs in order to serve as dispute resolution mechanisms under Safe Harbor. Therefore, the Department of Commerce cannot guarantee that a particular program will meet all Safe Harbor requirements, including those under FAQ 11).***", available at: http://www.export.gov/safeharbor/sh_workbook.html , last visited 23/02/04.

consumer associations. The various questionnaires that were sent out are included in Appendix IV. 5 DPAs, and the FTC did not answer the questionnaire so far.

4. Contextual Analysis of the SH Regime

This part of the study evaluates the impact on the SH Agreement of data transfer mechanisms adopted subsequent to SH in the EU and legislation adopted in the US. The legislative instruments under consideration have entered into force no later than November 3, 2003. In the case of the US, the study reviews relevant federal laws to assess the extent to which these regulations may affect the level of protection afforded by SH.

4.1. Impact of New Transborder Data Flow Regimes

4.1.1. Model Contractual Clauses

The European Commission has adopted two Decisions on Model contractual clauses after the adoption of the SH Decision (Decision 2001/497/EC concerning controller-to-controller data transfers; and Decision 2002/16/EC concerning controller-to-processor data transfers). Those Decisions may have a significant impact on transborder data flows to countries not assuring, as a whole, an adequate level of data protection. The study assesses the practical impact of the first Decision on the SH framework.

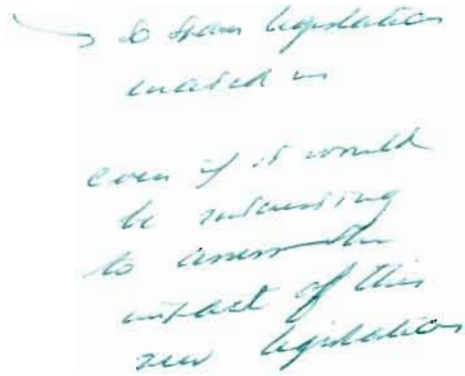
4.1.2. Binding Corporate Rules

The Article 29 Working Party has recently issued a Working Document on Binding Corporate Rules (BDR), which is relevant for the subject under study.[10] There are certain clarifications that may be relevant for the interpretation of the SH agreement as an instrument derogating from the general rule of Article 25(1) of the Directive. Moreover, point 5 of the Working Document elaborates on "Delivering Compliance and Guaranteeing Enforcement", which is indeed one of the main things to evaluate in the SH framework. This is relevant to make an assessment of the SH enforcement system in the light of certain core concepts expressed therein.

4.2. Impact of New US legislation

[10] Working Document no. 74 « Transfer of personal data to third countries : applying article 26(2) of the EU Data Protection Directive to binding corporate rules for international data transfers, 3 June 2003.

This part assesses whether and how certain new US legislation affect the level of protection provided for by the SH Principles.[11] Attention was given to the legal framework adopted after the events of September 11, 2001, as well as to any other sector specific Acts. Only legislation in force as of November 3, 2003 has been taken into consideration.



[11] It is relevant to make reference to what has been stated in relation to the Binding Corporate Rules : "Mandatory requirements of national legislation applicable to the members of the corporate group which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, are in principle not in contradiction with the binding corporate rules. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax reporting requirements or anti-money laundering reporting requirements. In case of doubt, corporate groups should promptly consult the competent data protection authority". Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU data Protection Directive to Binding Corporate Rules for International Data Transfers*, 3 June 2003, WP 74, p. 14.

III. Results of the Study

1. Theoretical Overview

1.1. Scope of Application

1.1.1. Geographic Scope of Application

According to Article 299 of the EC Treaty, the Treaty and thus all secondary legislation based on it, applies to the 15 Member States and the French overseas departments, the Azores, Madeira and the Canary Islands.[12] Secondly, the titel of the Commission Decision mentions that it is a text 'with European Economic Area (EEA) relevance'. The three EEA Member States, i.e. Norway, Iceland and Liechtenstein, are consequently bound by the Decision.[13] The transfer rules -- and thus potentially the SH arrangement -- apply to transfers conducted from those states.

The SH principles apply to US organizations who voluntarily subscribe. The Decision does not contain any specific definition of what must be understood by "US organization." However, Article 2 specifies that the Decision "concerns only the adequacy of protection provided in the United States under the Principles (...)." Apparently a US organization must be located in the US to qualify for SH.[14] For instance, an Argentinean subsidiary of a US organization can not enjoy the benefits of SH, which implies that the other transfer exemptions will apply.

1.1.2. Material Scope of Application

---

[12] However, the Council can by a qualified majority on a proposal from the Commission and after consulting the European Parliament, adopt specific measures aimed, in particular, at laying down the conditions of application of the present Treaty to those regions, including common policies. A partial exception exists for the °Aland Islands. The Treaty does not apply to the Faeroe Islands, the Sovereign Base Areas of the United Kingdom of Great Britain and Northern Ireland and Cyprus. The Treaty applies to the Channel Islands and the Isle of Man only to the extent necessary to ensure the implementation of the arrangements for those islands set out in the Treaty concerning the accession of new Member States to the European Economic Community and to the European Atomic Energy Community signed on 22 January 1972.

[13] Switzerland, while being a member of EFTA is not a Party to the EEA, having voted against membership in December 1992. Switzerland maintains and develops its relationship with the EU through broadened bilateral Agreements.

[14] This can also be deduced from the e-form published on the DOC website, http://web.ita.doc.gov/saveharbour/shreg.nsf/safeharbour?openform

1.1.2.1. Relevance of the FTC and DoT jurisdiction

The material scope of application of the SH principles is to an important extent determined by the jurisdiction of the FTC and the DoT. The SH regime applies only to sectors and/or data processing that fall under the jurisdiction of the FTC or the DoT.[15] To put it differently, an US Organization can qualify for SH regime, only if failure to comply with its statement to adhere to the principles is actionable under Section 5 of the Federal Trade Commission Act, prohibiting unfair and deceptive acts.[16]

* A deceptive practice is defined as a "representation, omission or practice that is likely to mislead reasonable consumers in a material fashion."[17] According to Annex III of the Decision, the FTC claims broad jurisdiction over misrepresentations about the collection and use of consumer data.[18] Consequently, an US organization that certifies for SH without factually respecting the regime may fall within the FTC's jurisdiction, since this would constitute a "deceptive practice" within the meaning of Section 5 of the FTC Act.[19] Accordingly, every entity that self-certifies its adherence to the DOC may fall within the scope of the principles.

Some nuances need, however, to be made:

First, Courts have not upheld thus far the FTC's broad claim of jurisdiction regarding privacy representations.[20] Although some cases may raise no doubt and constitute a deceptive practice,[21] other cases may figure in a gray zone and leave the controller as well as the data subject with uncertainty. Pursuant to 15 U.S.C. §45(n), a practice is deemed "unfair" if it *causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition.*[22] The control of the FTC is only marginal and allows to balance a commercial practice with the commercial benefits the data subject gets in exchange. Although processing practices must be assessed case-by-case, the FTC has in its letter to

---

15 See Recital nr. 6 of the Decision.

16 Or under each other law prohibiting such act.

17 A practice is unfair if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition, see letter to Mr. John Mogg, July 14, 2000.

18 The letter of FTC Chairman Pitofsky directed to Mr. Mogg, DG XV of the Commission gives the example of a web site that falsely claims to comply with a stated privacy policy or a set of self-regulatory guidelines. It is further stated that the "(FTC) has taken the position it may challenge particularly egregious privacy practices as unfair under section 5 if such practices involve children, or the use of highly sensitive information, such as financial records and medical records." See also FAQ 6 that considers that "Any misrepresentation to the general public concerning an organization's adherence to the SH Principles may be actionable by the Federal Trade Commission or other relevant government body. Misrepresentations to the DOC (or its designee) may be actionable under the False Statements Act (18 U.S.C.)."

19 Misrepresentations to the DOC (or its designee) may be actionable under the False Statements Act (18 U.S.C.), see FAQ 6.

20 See J.R. Reidenberg, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal*, Vol. 54 April 2003, p. 877 - 898

21 Geocities and ReverseAuction.com (Those cases have been settled by the FTC and they are not court decisions).

22 Own Italics.

the EC pointed out that "a company's failure to abide by a stated privacy policy is likely to be a deceptive practice."[23]

Secondly, the FTC's jurisdiction extends to unfair or deceptive acts or practices "in or affecting commerce." Personal data collected and processed by corporations that are promoting goods and services, including collecting and using data for commercial purposes, would presumably meet the "commerce" requirement.[24] However, there exists considerable doubt about the FTC's competence as regards the SH agreement.[25] Simarly, the FTC will in principle have no jurisdiction over the collection and use of personal information for non-commercial purposes or charitable fund-raising.[26] According to Annex III of the Decision, one should take into account the commercial character of the purpose of the data collection, rather than the commercial nature of the data controller.

Processing of personal data for purposes of employment or research activities (e.g. use of personal information for developing and testing drugs) would then not be covered by FTC jurisdiction and would ordinarily be outside SH. The FAQs contain nevertheless specific provisions concerning Human Resources data and transfers to the US for pharmaceutical research and/or other purposes. The EU Data Protection Working Party confirmed that there may be uncertainty as to whether personal data processed for these purposes would be covered by the SH requirements.[27]

* Section 5 of the FTC Act excludes the FTC's authority with regard to (1) financial institutions, including banks, savings and loans, and credit unions; (2) telecommunications and interstate transportation common carriers; (3) air carriers; (4) and packers and stockyard operators. These are mostly partial exceptions.

* Personal data processing operations conducted by organizations that come within the range of the DoT's jurisdiction can also certify for the SH Principles. The DoT can take enforcement based on section 49 U.S.C. 41712, which prohibits a carrier from engaging in "an unfair or deceptive practice or an unfair method of competition" in the sale of air transportation that results or is likely to result in consumer harm. Again, failure to maintain the privacy of information obtained from passengers would not per se constitute a violation of this section, but only if the organization has publicly committed to the principles.[28]

---

[23] See also Decision, Annex III

[24] Letter of FTC Chairman Pitofsky.

[25] "Indeed, in the past, the FTC has Stated to Congress that consumer unfairness requires substantial injury and that "emotional impact and other more subjective types of harm will not ordinarily make a practice unfair. Since all of the FTC's deceptive practices cases have settled prior to any court decision, the legal standards remain uncertain." See J.R. Reidenberg, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal*, Vol. 54 April 2003, p. 877 - 898.; J.R. Reidenberg, E-commerce and Transatlantic Privacy, Houston Law Review, ; Y. Poullet, "The Safe Harbor Principles - An Adequate Protection?", International Colloqium organized by IFCLA, Paris, 15-16th of June 2000, available at: http://www.droit.fundp.ac.be/textes/safeharbor.pdf, last visited 28/02/04.

[26] Decision, Annex III. The letter of FTC Chairman Pitofsky gives the example of a "chat room" operated by noncommercial entities, e.g. a charitable organization.

[27] The Article 29 Working Party pleaded to expressly exclude these categories of data transfers from the "SH," Opinion 7/99 p. 4-5

[28] See the letter of Mr. Samuel Podberesky, Assistant General Counsel for Aviation Enforcement and Proceeding, to the EC, Mr. John Mogg, Director, DG XV.

1.1.2.2. Transfers of "personal data"

The SH arrangement applies only to transfers of "personal data" or "personal information." Those categories are vaguely defined to include "data about an identified or identifiable individual that are within the scope of the Directive, received by a US organization from the EU, and recorded in any form."[29] This suggests that the same meaning of Article 2 (a) of Directive 95/46 should apply to the SH principles. The Directive defines the term "personal data" as "any information relating to an identified or identifiable natural person."[30]

Information that is rendered "anonymous" by an intermediary who can without unreasonable difficulty conduct a "reverse identification" will also fall within the scope of the Directive (so called "coded data"). There remains uncertainty whether the principles apply to such "coded data." With regard to "employment data" FAQ 9 excludes "anonymized" or "pseudonymized" data from the scope of application without further clarifying what these notions exactly mean. Furthermore, FAQ 14 regarding research data holds that a transfer from the EU to the US of data coded by the principal investigator would not constitute a transfer of personal data that would be subject to the principles. It is unclear if one could extent those limitations to the processing of other data categories under the SH regime.

More concretely, the question raises what should be understood by "anonymized" and "pseudonymized" data. There exists a continuum between clearly personal data and anonymous, non-traceable data; many categories of data fall in between these two extremes. In a transfer context, if there exists interdependence between transferor and transferee personal data likely will not entirely be "anonymized," unless anonymization would be guaranteed by a trusted third party. For instance, if a subsidiary based in the EU transfers employee data to its headquarters in the US after having replaced the names and addresses by an ad random number, would the transferee need to apply the principles? It is arguable that the exemption only covers those cases were there are sufficient guarantees

---

[29] See Annex I to the SH Commission Decision.

[30] An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." It is not necessary that data identify the data subject. The mere fact that data can be related to an identifiable or identified person suffices. To determine whether a person is identifiable, Recital 26 of the Directive specifies that one should consider "the means likely reasonably to be used either by the controller or by any other person to identify" the data subject. In the context of a medical research program, for instance, if a medical doctor replaces the personal identifiers of medical data sent to a pharmaceutical enterprise by an ad random number assigned by the computer, the Directive applies, since the supplier of the information, i.e. the doctor, can relate the data to a specific patient. The meaning of the words "the means likely reasonably to be used" is unclear. The reference is probably intended to cover only technical means. In practice, reversible coding may be supplemented by contractual restrictions (and sanctions) to prevent identification of individuals. Such restrictions make the use of technical means less likely and unreasonably and should thus be taken into account in determining whether data are personal data. Also, the cost of decoding is a factor that impacts on the likelihood of possible decoding; the higher the cost, the less likely decoding is.

that there exist enough safeguards preventing the key being send from transferor to transferee. If not, one could easily circumvent the principles by coding the identifiers.[31]

An "adequate level of protection" does not necessitate the endorsement of a definition of personal data that is identical to the definition of the Directive. Only if the impact of a narrower definition would burden the privacy and related freedoms of the data subject with an unacceptable risk would there be a problem. The SH text specifies that U.S. law will apply to questions of interpretation and compliance with the SH principles and relevant privacy policies by SH organizations, except where organizations have committed to cooperate with European DPA's (e.g. in the context of human resources transfers). Consequently, the interpretation of the FTC or DOC will be determining in the end. However, the SH framework contains a subtle system of checks and balances. If the US authorities' interpretation would erode the adequacy finding of the Commission, it can in accordance with Article 3(4) of the Decision readjust the principles. US organizations can in accordance with FAQ 5 co-operate with European DPA's in which case the interpretation of these authorities will prime.

1.1.3. Personal Scope of Application

The SH principles only apply to US organizations, without this term being defined. The semantics of the Decision let understand that the principles would not apply to individuals that receive personal data from the EU. However, natural persons who own and operate a business as a sole proprietorship or partnership that engages in data transfer, can be qualified as an organization eligible for certification. The FTC has on many occasions claimed jurisdiction over individuals when they have violated the FTC Act, imposed fines or entered into agreements with individuals. Only if these persons would not be within the scope of the FTC's or DOT's jurisdiction, could individuals not benefit from the arrangement.

The notion "US Organization" may not be interpreted by bluntly referring to the definition of "data controller" in the EU Data Protection Directive. The SH principles do not refer to the Directive as regards the definition of "US Organizations," and as has been indicated before, the principles generally fall under the interpretation of the US authorities, which margin of interpretation is being narrowed by the adequate level of protection requirement. This implies that a material criterion is imposed, rather than a procedural one (as in the Directive). Moreover, several hypotheses could be made with regard to the scope of the notion "US Organization":

---

31 "As data is aggregated in purportedly anonymous fashion and then used for demographic profiling, the aggregations compromise the ability of any single member of society to participate in decisions about the treatment of personal information. To the extent that profiles become more refined and more predictive, individuals will be stereotyped for particular behaviour and 'aggregate' data becomes associated with individuals," See J.R. Reidenberg, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal*, Vol. 54 April 2003, p. 877 - 898.

(i) A department that forms an integrated part of the same legal entity of a corporation likely does not constitute a separate organization under SH. For instance, if EU personal data held by a corporation is forwarded to one of its departments, this would not trigger the onward transfer rules because it may be argued that the information is only circulating within the same organization. To put it in the semantics of the Directive, the organization is a "controller" who determines the purposes and means of the processing, independent to the fact that the effective processing is realized by one of its departments;

(ii) If data is shared between various companies that are member of the same group the situation will be less evident, since legal criteria are missing to determine to what extent these companies constitute different "organizations". They likely constitute different "organizations," even more so if no specific processing guidelines would be imposed by the central management of the group.[32] The absence of such instructions would frustrate the adequate level of protection norm;

(c) An organization that, in the context of the SH arrangement, performs processing operations on behalf of an organization, is deemed to constitute a separate entity, to be distinguished from the "organization." Thus 'a processor' under the Directive may qualify as a 'third party' in the SH context, if it is acting as an agent to perform task(s) on behalf of and under the instructions of the organization.[33] The fact that a corporation has a contractual relationship with another legal entity, does not exclude that the latter must be qualified as a 'third party.' Alleging the contrary would excavate the principles. It can be deduced from a general reading of the principles that, the notion of 'third party,' although unclear, denotes another legal entity.

While the Directive pursues a functional approach, (i.e. the controller is defined by reference to his decisive powers he has regarding a data processing -purposes and means)[34], the SH arrangement seems to be based on a corporate law approach taking the 'legal personality' as a main criterion for delimitating "US organizations."

1.2. Actors involved

---

[32] It must be remarked that the Principles tend to connect an "organization" with a "separate legal entity," rather than with the decision making power on a specific processing. This can be deduced from FAQ 6 where it is stated that "*(a)n organization that will cease to exist as a separate legal entity* as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance (italics supplied).

[33] Note that a 'third party' does not *per se* mirror a 'processor' under the Directive, but only if that entity *performs tasks on behalf of and under the instructions of the organization*. It can already be remarked here that it is not necessary to apply the notice and choice principles when disclosure is made to such a third party. The Onward Transfer Principle, on the other hand will apply (see end notes to the Principles).

[34] The notions and definitions in the Directive have a certain 'functional autonomy,' as is the case with qualifications in continental criminal law. The Directive's terms have their autonomous logic in function of the goals that the Directive pursues.

The SH arrangement holds the middle between a self-regulatory scheme and rules enforced by public authorities and may be viewed in a certain sense as a co-regulatory scheme. The SH regime shows analogy with a state law regime since the principles have been adopted by the Commission. Analogous to State law, private entities have no or little autonomy as regard the substance of the principles, i.e. data controllers can not chose their own principles and can not go below the level of protection laid down by the principles. The principles show, however, more procedural autonomy than classic state regulation: (i) data importers are free to adhere to the principles; and (ii) enforcement can be handled by private enforcement programs. Further, it shows bi-cultural characteristics since it provides for a data protection regime implemented at both sides of the Ocean.

The complexity of the SH principles results in a multitude of actors. The relevant actors are the following:

1.2.1. Public Actors

12.1.1. European Public Authorities

a) Data Protection Authorities ("DPAs")

A prerequisite to a valid data transfer is compliance by the data exporter of the local data protection regulations. In addition, data subjects will primarily consider filing a complaint with a local DPA. National DPAs are entrusted with the tasks set forth by Article 28 of Directive 95/46, specifically with the monitoring of the application of the national data protection regulations. They can, in that context, use the powers described in Article 28(3) of the Directive, as specified by national law.[35] In certain member states, DPAs may impose administrative sanctions. In other member states, DPAs may investigate data processing activities and refer the complaint/file to the Public Prosecutor if (i) a violation of the data protection law is established, and (ii) such violations are criminally sanctioned.

DPAs may be empowered to block data streams in application of Article 3 of the SH Decision[36] (the "Decision").[37] Pursuant to this provision DPAs may suspend data flows

---

[35] These powers include: (1) investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties; (2) effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions; and (3) the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

[36] Commission Decision of July 26, 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the SH privacy principles and related frequently asked questions issued by the US Department of Commerce, O.J. L 215, August 25, 2000.

to an organization that has self-certified its adherence to the SH principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data (i) if the FTC or DoT, and/or independent recourse mechanisms (i.e. private sector developed privacy programs that incorporate the SH principles with associated enforcement mechanisms[38]) have determined that the US data importer is violating the SH principles implemented in accordance with the FAQs; or (ii) if there is a substantial likelihood that the principles are being violated.[39]

b) DPA panel (FAQ5)

US organizations may commit to cooperate with European DPAs, as set forth in FAQ no. 5 (such co-operation is a prerequisite for the valid transfer of human resources data under the SH framework). The panel, which exist of a number of DPA representatives may advise US organizations on unresolved complaints from individuals of personal data transferred to the US under the SH pursuant to the procedure laid down in FAQ 5. Failure to comply with the panel's "advice" may constitute a deception or misrepresentation under the FTC Act. Companies must undertake to comply with the Panel's advice.[40] Pursuant to FAQ 5 the Panel's functions are to provide (i) for a harmonised and coherent approach for assuring compliance with the SH; (ii) advice to the US organizations on unresolved complaints from individuals about the handling of transferred personal data; (iii) follow-up for referrals from organizations and/or individuals.

There have yet not been any enforcement actions by the DPA panel.[41]

c) Public Prosecutors

Public prosecutors are charged with the criminal enforcement of the national data protection regulations. Violation of national data transfer provisions are typically criminally sanctioned. Data subjects generally may also file a complaint with the public prosecutor's office in parallel with the DPA in case the data exporter would violate the data protection regulations prior to or during a data transfer.

d) Courts (criminal and civil)

---

37 Article 3 of the Decision uses the notion "competent authorities," and this power may be exercised by different authorities depending on how national law is structured.

38 See FAQ no. 11

39 This is the case only if (i) there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; (ii) the continuing transfer would create an imminent risk of grave harm to data subjects; and (iii) the competent authorities in the member state have made reasonable efforts under the circumstances to provide the organization with notice and an opportunity to respond.

40 See FAQ no. 5

41 http://forum.europa.eu.int/Public/irc/secureida/safeharbor/home

Civil and criminal courts have authority to decide on data exporter's compliance with local data protection regulations, and may, depending on the particulars of national law, block data streams pursuant to Article 3 of the Decision.

e) European Commission

The European Commission observes the following tasks :

- *Co-ordination of information*: Member states that block data flows are required to inform the Commission.[42] Member states and the Commission inform each other about any failure of private US enforcement mechanisms;[43]

- *Notification of the DOC and/or modification of the Decision in case of compliance failures*: if the Commission has evidence that 'any body responsible for ensuring compliance with the SH principles (...) is not effectively fulfilling its role, the Commission is required to inform the US DOC and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46 with a view to reversing or suspending the present Decision or limiting its scope;[44]

- *Evaluation of the SH principles*;[45]

- *The Commission may present draft measures.*[46]

f) Article 29 Working Party and the Article 31 Committee

The Article 29 Working Party delivered opinions on the level of protection provided for by the SH in the US which have been taken into account for the drafting of the Commission Decision.[47]

---

42 Article 3(2) of the Decision.
43 Article 3(3) of the Decision.
44 Article 3(4) of the Decision.
45 Article 4(1) of the Decision.
46 Article 4(2) of the Decision.
47 Recital no. 10 of the Decision. See Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government; 26 January 1999 (WP15); Opinion 2/99 on the adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999, 3 May 1999 (WP 19); Opinion 4/99 on the frequently asked questions to be issued by the US Department of Commerce to the proposed "Safe Harbor Principles", 7 June 1999 (WP21); Working Document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles", 7 July 1999 (WP 23); Opinion 7/99 on the level of data protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions

The Article 31 Committee will review the SH implementation report on it.

1.2.1.2.US Public Authorities

a) the FTC/DoT

Data transfer under the SH regime are permitted only if the data importer's failure to comply with the principles constitutes a misrepresentation or deceptive act which is actionable under Article 5 of the US Federal Trade Commission Act. The same applies to acts that are actionable under Title 49 United States Code Section 41712. SH data transfers are valid only if they are conducted within the FTC's and the DOT's jurisdiction, and private SH recourse mechanisms will refer the case to the FTC/DOT if the complaint can not be settled.

So far, there is no evidence that the FTC/DOT has undertaken enforcement actions.

b) State 'Unfair and Deceptive Practices' Authority

The SH overview's annex III refers to Unfair and Deceptive Practices Authorities at the State level ("mini-FTCs"). Violation of Article 5 of the FTC Act may also constitute a violation of State level Unfair and Deceptive Practice laws.

c) The US Department of Commerce (the "DoC")

The DoC negotiated and developed the SH principles with the European Commission. US organizations must certify annually their adherence to the SH principles with the DoC. The DoC keeps a register with SH members that is publicly available. The DoC further coordinates and documents the entire registration process for US organizations.[48] The DoC has pointd out that "*In maintaining the list, the Department of Commerce does not assess and makes no representation as to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.*"[49]

(FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce, 3 December 1999 (WP27); Opinion 3/2000 on the EU/US dialogue concerning the "SH" arrangement, 16 March 2000 (WP 31); Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles," 16 May 2000; and Working Document on Functioning of the Safe Harbor Agreement, 2 July 2002 (WP 62).

[48] http://www.export.gov/safeharbour/sh_overview.html ,last visited: 27/11/03.

[49] Italics added by the DOC, see: "Safe Harbor Workbook", available at: http://www.export.gov/safeharbor/sh_workbook.html , last visited 23/02/04.

d) US Courts

Data subjects may introduce a claim for a violation of the SH principles before US civil courts to obtain damages. However, data subjects will likely be successful only if they base their claims on breach of contract, *i.e.* in circumstances where acceptance of a privacy policy may be considered to constitute contractual rights and obligations. Costs of such action is typically very expensive and generally not affordable to data subjects.

1.2.2. Private Actors

2.1.2.1 European Private Actors

a) Data exporter

The data exporter will, pursuant to EU data protection law, be a data controller, *i.e.* a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.[50] Data processors, *i.e.* entities acting on behalf of the data controllers, and on the latter's instructions, can export personal data, only if the data controller has given such instructions.

Data exporters need to comply with the local data protection regulations to transfer personal data to a US SH organization. They will generally be the interface between data subject and the US data importer to handle data subjects' privacy concerns and/or complaints.

b) Data subject

The SH principles primarily concern personal data which is sent to the US by EU based data exporters. Although individual's nationality is not a relevant criterion to decide whether personal data is protected by the principles, SH data transfers will generally concern European data subjects (this is not necessarily the case, for instance, if personal data of a Chinese citizen is transferred from a European database to the US under the SH regime). US organizations, may of course use the principles to leverage their privacy practices and also apply to principles to data pertaining to US nationals (or other). Data subjects generally will be natural persons, SH covers individuals not legal persons

[50] Article 2(d) of the Directive.

2.2.2.2 US Private Actors

a) Data importer (US organization)

Data importers are US organizations. The notion of US organization is not defined by the principles. Part 1.1.3. on the personal scope of the principles analyses this question in more detail.

b) Data importer's agent

US organizations may use a "third party that is acting as an agent."[51] An agent is analogous to a data processor under Directive 95/46. Agents may receive personal data only if the US organization ascertains that the agent subscribes to the principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that it provides at least the same level or privacy protection as is required by the relevant principles. The US data recipient may also be a data processor of the EU based data exporter, in which case FAQ no. 10 applies.

c) Onward transferee

Onward transferees may be (i) other US organizations that are considered "data controllers" under EU data protection law; or (ii) agents or data processors.

d) Privacy Programs and Alternative Dispute Resolution Bodies (ADRs)

Organizations may chose to adhere to a privacy program as a means to comply with the Enforcement Principle.[52] These programs are "private sector developed privacy programs that incorporate the SH Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle."[53] Depending on the type of privacy program, adherents may have latitude as to the modalities of implementation of the SH, or will need to respect rules specified by the privacy program service provider for specific data processing applications (for instance, online customer data processing rules which specify the SH requirements to a specific data processing scenario). ADRs provide only for dispute settlement procedures without specifically requiring companies to implement privacy rules. In the context of data protection

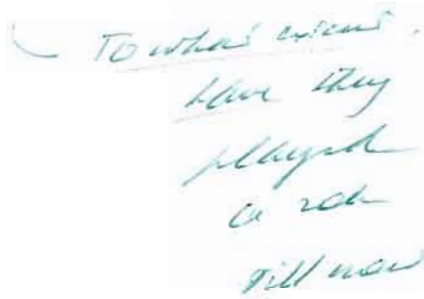
---

51 See the Onward Transfer principle.
52 FAQ no. 11
53 Idem.

complaint handling, it is essential that such services are affordable and transparent to the data subject.[54]

e) Business Representatives and Intermediate Organizations

Business representatives and intermediate organizations may also have an important role in the SH. They may provide for the institutional framework to develop and enforce privacy programs. Business organizations are important to inform member organizations of their obligations and to offer concrete tools and mechanisms to comply with the SH. For instance, the rules and principles set forth in the SH may be translated in codes of conduct to which member organizations represent to adhere. They may also engage in complaint handling and have the organizational means to effectively sanction member organizations in case of violations.



[54] FAQ no. 11 : "[...] As required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organizations operating the recourse mechanism, but such requirements should be transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints [...]."

2. Certification Page Analysis

This part provides for a factual analysis of representations made by SH companies on the DoC Certification page. All of the US organizations that were listed on the DoC SH certification list on 3 November 2003 have been reviewed.[55] At that date, 401 companies declared to adhere and implement the SH principles.

The paragraphs below summarize the factual findings which are tabled and visualized in the charts attached in Appendix V. Data has been collected on the following parameters:

1. Industry sector information: exhaustive overview of all the industry sectors represented by the companies importing EU information under the SH agreement;

2. Data categories: roughly classification of the various sectoral data categories of personal data transferred under the SH regime as declared in the box "Personal Information Received from the EU";

3. Personal Data Covered: on-line, off-line, manually processed, and/or human resources: ;

4. Controller-to-Controller, and Controller-to-Processor data transfers;

5. Data privacy policy location accuracy: assessment whether companies provide for an accurate and/or direct link to the relevant data privacy policy from the certification webpage;

6. Verification type: distinction between in-house and third party verification;

7. Regulatory body: this parameter indicates whether the SH adherent falls under the FTC or DoT jurisdiction, or whether they have erroneously mentioned the FTC as having jurisdiction (considering that they import human resources data);

8. Privacy program: this parameter indicates the various "privacy programs" that have been mentioned on the companies' certification pages;

9. Dispute resolution mechanisms/programs: this parameter indicates the various dispute mechanisms/programs that companies have mentioned on their certification page;

10. Co-operation with EU Data Protection Authorities: this parameter indicates companies' willingness to co-operate with EU Data Protection Authorities; *and*

[55] http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

11. Certification status: this parameter indicates the certification status (current/not current).

The results of the review are as follows:

2.1. Industry Sector Information

The participating companies belong mainly to the IT sector (51% in total):

- 16%: CSV (Computer Services)
- 13%: INF (Information Services)
- 12%: CSF (Computer Software)
- 6% : GSV (General Services)
- 4% : ADV (Advertising Services)
- 49%: others
-

The complete list of services as classified in the DoC's website is as follows:

- ACE: Architectural/Construction/Eng Svc
- ACR: Air Conditioning & Refrigeration Eq.
- ACT: Accounting Services
- ADV: Advertising Services
- AGC: Agricultural Chemicals
- AGM: Agricultural Machinery & Equipment
- AIR: Aircraft and Parts
- APP: Apparel
- APS: Automotive Parts & Service Equipment
- ARW: Artwork
- AUT: Automoviles & Light Trucks/vans
- AUV: Audio/Visual Equipment
- AVS: Aviation Services
- BOK: Books & Periodicals
- BTC: Biotechnology
- BUS: Business Equipment (other than computers)
- CEL: Consumer Electronics
- COL: Coal
- CON: Construction Equipment
- COS: Cosmetics & Toiletries
- CPT: Computer & Peripherals
- CRM: Ceramics Fine Advanced
- CSF: Computer Software
- CSV: Computer Services
- DFN: Defense Industry Equipment
- DRG: Drugs and Pharmaceuticals
- EDS: Education and Training

- EIP: Electronic Industry Prod/Test
- ELC: Electronic Components
- ELP: Electrical Power Systems
- EMP: Employment Services
- FLM: Films Videos & Other Recording
- FNS: Financial Services
- FOD: Foods Processed
- FOT: Footwear
- GCG: General Consumer Goods
- GFT: Giftware
- GIE: General Industrial Equipment & Supplies
- GST: General Science and Technology
- GSV: General Services
- HCG: Household Consumer Goods
- HCS: Health Care Services
- ICH: Industrial Chemicals
- INF: Information Services
- INS: Insurance Services
- INV: Investment Services
- LAB: Laboratory Scientific Instruments
- LES: Leasing Services
- MCS: Management Consulting Services
- MED: Medical Equipment
- MTL: Machine Tools & Metal Working Equipment
- MUS: Musical Instruments
- OGM: Oil & Gas Field Machinery
- OGS: Oil Gas Mineral Production/Exp Srv
- OMS: Operations & Maintenance Services
- PAP: Paper & Paperboard
- PCI: Process Controls Industrial
- PHT: Photographic Equipment
- PMR: Plastic Materials & Resin
- PRT: Port & Shipbuilding Equipment
- PUL: Pulp & Paper Machinery
- PVC: Pumps Valves & Compressors
- REQ: Renewable Energy Equipment
- RRE: Railroad Equipment
- SPT: Sporting Goods Recreational Equipment
- TEL: Telecommunication Equipment
- TES: Telecommunications Services
- TOY: Toy & Games
- TRA: Travel and Tourism Services
- TRK: Trucks, Trailers & Buses
- TRN: Transportation Services (Except Aviation)
- TXF: Textile Fabrics

2.2. Data Categories

The analysis of this parameter is based on the certification pages' entry named "Personal Information Received from the EU." Personal information could be roughly reduced to the following categories:

- C: Commercial (data used for advertisement purposes, in pre- and contractual relations, after sale services, etc.)
- HR: Human Resources
- RE: Research (including market research)
- T: Travel
- M: Medical
- RH: This category was included to refer to companies that represent to receive HR data from the EU in the item "Human Resource Data Covered," but did not make such a representation in the entry "Personal Information received from the EU".

Many companies do not define the categories of "Personal Information received from the EU", but explain how data is processed, the purpose, the business model, etc. In those cases, the data categories were inferred from the processing model description to the extent possible.

The approximate results of representations are as follows:

- Nearly half of the data type is Commercial data;
- More than one third concerns Human resources data[56];
- The remaining minority concerns Research data, Travel data and Medical data.

2.3. Controller/Processor

It must be remarked that the number of organizations that import personal data in a data processor capacity may be higher in reality, since the distinction between controllers and processors is not necessarily indicated on the certification page, and may appear only from the privacy policy.

11% of the companies have declared to import personal information in a data processor capacity. The other 89% must be considered data controllers.

[56] This includes the companies (9%) that did not specify this data type under the item "personal information received from the EU," but answered positive under the item "personal data covered". These are the companies that scored "RH".

2.4. Personal Data Covered

The results are as follows:

- 37%: on-line data
- 25%: off-line data
- 21%: human resources data
- 17%: manually processed data

The distinction between these four categories is set forth on the DoC certification page. It must be noted that this page blends a data type, with data processing modalities (online, offline and manually).

2.5. Privacy Policy Location Accuracy

Companies adhering to the SH agreement must specify in the certification page or letter where the privacy policy is made publicly available. Normally they include a hyperlink to their privacy policy. However, the hyperlink sometimes lead to companies' homepage and not directly to the privacy policy.

Certain companies give sometimes a physical address where the privacy policy is supposed to be available, or they mention "Available Upon Request." It has to be taken into account that those categories do not *per se* mean that the location is accurate, or that they are truly available to the public. Only in the context of the in-depth analysis were such companies contacted by e-mail (see *infra*, part [ ]).

The categories, then, are the following:

- Y: Yes (the hyperlink given in the certification page does work and leads directly to the relevant privacy policy);
- No: No (the hyperlink given does not work or no link was given;
- NDL: No Direct Link (the link provided did not lead directly to the privacy policy but to the homepage. It was necessary to search in the company's website to find the policy);
- PA: Physical Address (they give a physical address as location);
- Intranet: they express that the privacy policy is located at the company's Intranet); *and*
- AUR: Available Upon Request

The following results were scored:

- 40% of the companies provided a hyperlink in the certification page which directly leads to the relevant privacy policy;
- 33% of the companies did not provide for a direct link to a relevant privacy policy but to the homepage;
- 13% did not provide any hyperlink or the one provided did not work;

- 6% of the companies declared that the policy is available on their intranet;
- 5% of the companies certify that the policy can be obtained at a physical address ; *and*
- 3% have specified that the policy is available upon request.

2.6. Verification

- 86% of the SH companies opt for in-house verification.
- 14% choose a third party verification mechanism.

2.7. Regulatory body

All except one company represented to be falling under the jurisdiction of the Federal Trade Commission (FTC). One US organization represented to be regulated by the Department of Transportation (DoT). However, organisations importing human resources data scored "error", because the FTC jurisdiction on human resources data is doubtful. Organizations that represented to import both human resources data and non-human resources data scored "both." As a consequence, approximately half of the companies that represent to import human resources data doubtfully fall under FTC jurisdiction.

2.8. Privacy Program

The SH does not provide for a positive definition of privacy program. However, the concept can be deduced from FAQ 11 where it says that privacy programs have to "(i) incorporate the SH principles into their rules, and [that] (ii) include effective enforcement mechanisms of the type described in the enforcement principle." Privacy programs must be distinguished from mere dispute settlement programs or services which do not set forth substantial privacy requirements. While most companies do not adhere to a privacy program, some do. It must be observed that little of the items mentioned below can be considered privacy programs. The following chart indicates the organizations that have been certified as a "privacy program," whether true (privacy program) or false.

AAA: American Arbitration Association
AABB: American Association of Blood Banks
AIM : Association for Interactive Marketing
ASISP: American Society for Industrial Security's Privacy
BBB: BBBonline
BNI: Business Network International
BR: The Belmont Report
CASRO: Council of American Survey Research Organizations
CAUCE: Coalition Against Unsolicited Commercial E-mail
CFR: The Code of Federal Regulations

CIDE: Chemical Industry Data Exchange
CLSR: Center for Legal and Social Responsibility
CNIL member: "We registered our privacy policy to the Commission Nationale de l'Informatique"
COPPA: Children Online Privacy Protection Act
CRe-m: Council for Responsible e-mail
CSPSTI: Cyber Security Data Exchange
DHHSFAPHS: The Department of Health and Human Services Federalwide Assurance Protection for Human Subjects
DMA Privacy Promise
DMA: Direct Marketing Association
DMACFCRe-mail: Direct Marketing Association Council for Responsible e-mail
DMAgui: Direct Marketing Association Guidelines
DMAshp: Direct Marketing Association SH Program
DoC: US Department of Commerce SH Program
DPA for Human Resources
EPOF: European Privacy Officers Forum
EPON: European Privacy Officers Network
ESRBPOP: Entertainment Software Rating Board
GBCC: The Greater Boston Chamber of Commerce
GHEI: Guidelines for Handling Employee Information
HIPPA: Health Insurance Portability and Accountability Act
HON: Health on the Net
IAPO: International Association of Privacy Officers
IOPO: International Organization of Privacy Officers
KPMG: KPMG Security Seal
MRA: Marketing Research Association
NAI: Network of Advertising Initiative
NAITA: North Alabama International Trade Association
OPA: Online Privacy Alliance
P3P: Platform for Privacy Preferences
PAB : Privacy and American Business
PIMC: Personal Information Management Council
PrivacyBot
SHRM: Society for Human Resources Management
SSN: Secure Site Network
TPC : The Privacy Concil
TRUSTe

The scores for adherence to SH privacy programs is as follows:

- 53% of the organizations are not member of a SH privacy program;
- 14% of the organizations is member of TRUSTe;

- 6% of the organizations represents to adhere the DMA privacy (or SH privacy) program;
- 5% of the organizations is member of BBBonline.
- 22%: others

2.9. Dispute resolution mechanisms/programs

The participating companies should, in their self-certification letter, mention the independent recourse mechanism that is available to investigate unresolved complaints.

The following programs/services were mentioned whether they are or not ADRs:

DPA: Data Protection Authority
DMAshp: Direct Marketing Association Safe Harbour Program
DMA: Direct Marketing Association
TRUSTe
BBB: Better Business Bureaus
AAA: American Arbitration Association
HON: Health On the Net
USERTRUST
ESRBPOP: Entertainment Software Rating Board
Eftpeb: Exception for third party enforcement body
JAMS: Judicial Arbitration and Mediation Service
CFO
OR: online resolution
WWTS: SH Team at World Wide Travel Service

The scores for the most relevant categories are :

- Almost two third of the companies represent to co-operate with the DPA panel
- Less than a fifth of the companies are member of TRUSTe membership
- Less than 10 % of the companies are member of BBBonline membership
- Less than 10% is member of the DMA (without specification to implement the DMA SH programme)
- Less than 5% represented AAA dispute resolution
- Less than 5% adheres to the DMA SH programme

2.10. Cooperation with EU Data Protection Authorities

- 73% of the US organizations certified their willingness to co-operate with the EU DPAs;

- 27% scored negative.

Further to that, it must be observed that within the negative class of 27%, 5 companies (appr. 1% of the companies) import human resources data, for which cooperation is mandatory.

2.11. Certification Status

- 94% of the certifications are "current;"
- 6% are "not current".

put in the conclusion: what happened with the data already transmitted and company is not current any more and can be taken out of the list.

3. In-depth Implementation Analysis of SH

3.1. Visible Indicators and Trends on Compliance/Implementation

This section describes the results of the analytical analysis and identifies some indicators and trends as regards the implementation of the SH regime.

3.1.1. Analysis of Adherent Organizations

As indicated above sub. II. Methodology, the assessments concerns 10% (41 companies) of the organizations that have self-certified as of November 3, 2003. Within that sample, 29% of the organizations (12 companies) did not make their privacy policies available on the web. As a consequence they have been scored "unknown" for the substantive criteria. 11 of those 12 companies certified that they import human resources data. That means that, strictly speaking, the privacy policy has to be made available to these organization's employees (data subjects concerned). Thus, the fact that the privacy policy was not available online did not necessary result in a negative score for these companies. However, an e-mail was sent to these companies (8) asking for an available copy of the policy.

While it is not possible to give statistical significance to the outcomes with such a high "unknown" rate, the SH regime requires 100% compliance with every criteria since all its criteria/principles are essential to guaranteeing adequate protection.

The results function as valid indicators of general SH compliance and show trends as regards the implementation of the SH principles. The report utilizes below the notions "Neutral Indicators", "Organizations' Compliance Indicators" and "General Trends." The "Neutral Indicators" describe the categories that may show certain factual data, but concerning which a compliance analysis can not be made since they have no positive normative (or mandatory) value pursuant to the SH framework. "Organizations' Compliance Indicators" describes findings dealing with mandatory SH requirements. "General Trends" provides for initial findings derived from the indicators, illustrated by certain significative examples.

It appears from the made representations that 7 companies import personal data as "processors", and 1 both as "controller-processor". The "processors" are not taken into account for the item "Organizations' Compliance Indicators", and they scored "Not applicable". Each "controller-processor" was analysed in its "controller" capacity. Whereas the certification criteria have been analysed for all 41 companies, the substantive and enforcement criteria have only been analysed for those companies that import personal data as a data controller. That means that the assessment of the certification criteria, 41 companies have been taken into account (both data processors and controllers), while the assessment of the substantive and enforcement criteria considered

34 companies (data controllers only). It has to be taken into account that certain requirements are not always mandatory for every company.

A. Neutral Indicators

- Approximately half of the organizations **publicly disclosed their privacy policy** on the web. The policies of 6 companies were not publicly available on the web: 5 organizations certified to have their policy published on their intranet, 3 certified that the policies were available at a given physical address, and 6 organizations did provide for erroneous hyperlinks. 7 companies made publicly available a privacy policy that covers only partly the data processing indicated on the certification page. For instance, the privacy policy covers only data collected on an organization's website (i.e. online data), while the certification page represented that the organization processes also human resources data, manually processed and/or online data. E-mails have been sent to those companies representing a physical address and intranet as the location for their privacy policies. Of the 8 e-mails sent 3 answers have been received with the privacy policy in attachment;

- Slightly more than half of the organizations' **privacy policies were published on the web in a printable format**. For approximately one quarter of the policies it was not possible to determine whether they are printable or not since they were not posted on the website. The remaining companies published a privacy policy covering only part of the certified data streams;

- The great majority of the organizations **represented to use the SH principles for specific data streams**, while a limited number of companies did not restrict the personal data covered (these organizations used the principles for online data, offline data, human resources and manually processed data);

- Approximately one fifth of the reviewed privacy policies showed that the SH framework is used to send personal information to US organizations in their **capacity of data processors**. A very small minority are acting both as data controller and processor (with respect to different data streams), while the remaining companies are importing personal information exclusively as a data controller;

- Approximately three quarters of the SH organizations have made no representation concerning any **US law preventing compliance** with the SH principles. Some of them made general references to the obligation to cooperate with law enforcement agents;

- More than one third of the companies participate in a **privacy program**;

- Nearly all of the companies have chosen an in-house **verification method**;

- More than half of the companies have chosen the DPAs as **independent recourse mechanism**. The order of the selected private sector recourse mechanisms is as follows: first TRUSTe, second DMA (non-specific SH program), third AAA, fourth BBBonline, and last DMA SH program;

- Nearly half of the companies use the SH principles for importing **human resources data**;

- Approximately three quarters of the companies have decided to **co-operate with the European Data Protection Authorities** (this does not imply that these companies accept to implement a decision of a DPA *(per se)*. It has to be noted that not all of them have represented to cooperate with the DPAs in their privacy policy. Less than one fifth had made such a representation in their privacy policies.

- Less than half of the organizations described the **personal data type** received from the EU. More than one third did not describe the type of processed EU data. Approximately one fifth provided for a description that is unclear.[57]

- Nearly half of the companies represented **third party disclosures**. One quarter scored "unclear", while a minority did not represent to disclose personal data to third parties. One quarter scored "unknown";

- More than one third of the companies did not give **notice for secondary use**. Approximately one third provided such notice. One quarter scored "unknown".

- Approximately three quarters of the companies have chosen to provide **independent recourse mechanism pursuant to FAQ 5** (DPAs).

B. Organizations Compliance Indicators

1. Elegibility indicators

- Approximately half of the companies represented that they may **make changes in the policy**. Approximately one fifth do not make a representation to that effect. Approximately one quarter scored "unknown".

- Approximately one third of the companies provided for an **accurate location** of the privacy policy from the DoC certification list. Approximately one third did not

[57] FAQ 6 sets forth that "to self-certify for the SH, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the SH, that contains at least the following information: [...] 2. Description of the *activities* of the organization with respect to personal information received from the EU. [...]."

provide for an accurate location. One quarter scored "unknown". A minority of companies scored "yes/no" because the privacy policy that was accurately located covered only a part of the certified data streams.

- Approximately one fifth of the companies did not state the **specific statutory body that has jurisdiction to hear claims against the organization**. They are companies importing human resources data and they make a doubtful statement in the certification letter since the FTC has no jurisdiction over human resources data. Another fifth of the companies import human resources data and other kind of data as well, so, they have scored "yes/no". More than half of the organizations did correctly specify the FTC as the regulatory agency.

2. *Substantive indicators*

- Less than half of the companies **specified the purpose** of processing activities. More than one quarter expressed it in an unclear fashion. Approximately one quarter scored "unknown".

- Approximately two third of the companies included **organization contacts** in their privacy policy. A small minority did not include contact information. The remaining scored "unknown".

- Nearly half of the companies provided **notice of choice for use**. Approximately one fifth of the companies provided notices in an unclear manner or did not provide choice at all. Approximately one third scored "unknown".[58]

- Approximately two thirds of the companies did explicitly state in their relevant published privacy policy that they **adhere to the SH Principles**. A small minority did not make such a declaration. The remaining organizations scored "unknown".

- Only 8 companies represented to import **sensitive data**. 1 company did not represent to provide opt-in for sensitive data, and 2 made unclear representations regarding opt-in. Another 5 companies represented to provide opt-in.[59]

- Approximately half of the companies represented to adopt **reasonable security measures**. Approximately one quarter of the companies did not represent to provide for security measures or made an unclear representation. The remaining scored "unknown".[60]

---

58 Figures based on 21 companies.

59 Figures out of a total of 16 companies since only data controllers that represented to import sensitive data were taken into account here.

60 Figures out of 41 companies.

- Approximately one third of the companies expressed the **notice in an unclear manner**. Less than half of the companies expressed it clearly. The remaining scored "unknown".

- Approximately half of the companies expressed **notice in a conspicuous manner**. Approximately a quarter of the companies did not express it conspicuously. The remaining scored "unknown".

- Less than half of the companies did not provide **notice of choice for dissemination of personal data to third parties,** or did not provide it in a clear manner. One third did provide such notice, and the remaining scored "unknown".[61]

- More than one third of the companies did not provide **clear notice of choice for use and dissemination**. Less than one third did give such notice of choice. The remaining scored "unknown".

- Approximately half of the companies provided for a **conspicuous notice of choice for use and dissemination**. Approximately one fifth did not. The remaining scored "unknown".

- More than half of the **notices of choice** were not **readily available**. A minority were readily available. The remaining scored "unknown".[62]

- Nearly two third of the reviewed policies did not make representations regarding **affordability of choice**. The remaining scored "unknown".[63]

- More than one third of the companies did not represent their **third party processor's commitment to respect the SHA**. Approximately one quarter did give such information. The remaining scored "unknown".[64]

- Approximately half of the companies ambiguously specified the **relevance of the data for the specified purpose** ("unclear"), or did not specify it at all. A minority expressed it clearly, and the remaining scored "unknown".

- Nearly half of the companies did not (or did not clearly) represent the adoption of any **steps to ensure reliability for the intended use**. Approximately one third represented to take such steps. The remaining scored unknown

- Approximately half of the companies did not provide for **reasonable access**, while one quarter did provide access and the remaining scored "unknown".

---

61 Figures based on 30 companies
62 Figures based on 26 companies.
63 Figures based on 26 companies.
64 Figures based on 25 companies.

- Approximately two thirds of the reviewed policies represented that **cost for access** is reasonable/affordable, or free.

- Approximately half of the companies represented to offer an opportunity for correction or amendment. Approximately one third of the companies did not provide for the possibility to make **correction/amendment** of inaccurate data, or made unclear representations. The remaining scored "unknown".

- Approximately half of the companies did not provide for the possibility to **deletion of inaccurate data** or made unclear representations. Approximately one quarter provided for that possibility, and the remaining scored "unknown".

3. Enforcement Indicators

- Almost two third of the companies have represented to **cooperate with the DPAs** only in the DoC certification page. Approximately one fifth have represented their cooperation in both the certification page and the privacy policy. The remaining quarter did not represent to cooperate with the DPAs.

- More than two third of the companies did not agree to **comply with the advice** of the DPAs. Less than 10 % (2 companies) agreed to comply with DPA advice. The rest scored unknown.

- None of the companies has elected an **US legal or regulatory supervision body other than the FTC**.[65]

- All of the companies have represented to opt for **independent recourse mechanisms**.[66] All of these mechanisms are readily available because it concerns (1) the DPA panel; and (2) all ADRs chosen by companies are **readily available**.

- Less than half of the companies transparently set forth a dispute resolution procedure in their privacy policy, while less than half did not transparently mention or describe such procedures. The remaining scored "unknown."

- Nearly three quarters of the companies did not agree to **reverse the effects of a breach**, or expressed their agreement in an unclear manner. A minority offers reversal, and the remaining scored "unknown".[67]

- Nearly three quarters of the companies have not represented or do not adhere to a dispute resolution proceeding that foresees a remedy that result in **future**

---

65 See FAQ no. 11.

66 Further research is needed to determine whether these mechanisms are effectively independent by analyzing concrete decision-making.

67 Idem

processing in conformity with SH. A minority did offer such a remedy, and the remaining scored "unknown."

- Nearly three quarters of the companies did not represent as a remedy that the processing of the personal data may be **ceased**. A minority did offer such a remedy and the remaining scored "unknown".[68]

- More than three quarter of the companies did not include in their sanctions **the publicity for findings** of non-compliance or scored "unclear". A minority provides for a publication measure, and the remaining scored "unknown".[69]

- Less than half of the companies did not provide for **sanctions** either in the privacy policy, or through the ADR entity chosen. More than one third represented sanctions or a sanction regime, and the remaining scored "unknown".[70]

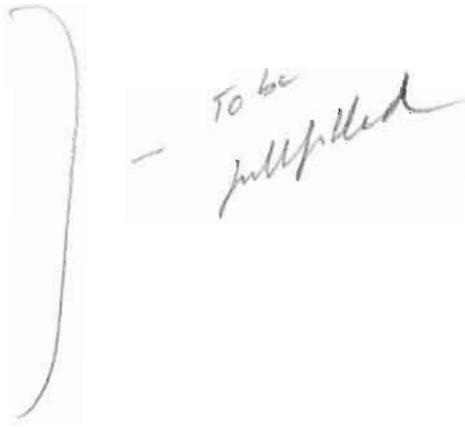
3.1.2. Analysis of Privacy Programmes and ADRs Bodies

A. Neutral Indicators

B. Programs and ADRs' Compliance Indicators

4. Substantive indicators

5. Enforcement indicators



3.2. Specific case-study

This item can not be develop for the moment since only one answer has been received so far.

3.3. ADR/ODR

[68] Idem
[69] Idem
[70] Idem

So far only one answer has been received of an ADR service provider.

3.4. Implementation experience by different parties

a) Lawyers

The questionnaire, attached to the report in Appendix IV, was sent to 15 lawyers- data protection experts, practising in the EU and in the US. We have received) answers. For reasons of confidentiality the answers are rendered anonymous:

1) In what concerns the **advantages** of the SHA regime lawyer A has answered: "SH has a number of advantages, in particular 1) broad coverage of (potentially) many types of data transfers to the US, 2) not requiring individual, ad hoc measures for each transfer (as is the case with the model contracts), 3) liberal rules concerning onward transfers, and 4) localization of the enforcement risk in the US (which also has a negative side, see the next question)."

Lawyer B has said: "Subscribing to SH means a solution for *all* future data transfers to the SH company in the United States. As for the affiliation to SH, the company can basically forget the prohibition on data transfers because after SH, the company becomes "safe" and outside the scope of the prohibition. So, the advantage is that it is not necessary to ascertain on an ad hoc basic which legal grounds for transfer to such a company will be used because the SH provides for a unified solution for *all* the existing and forthcoming transfers." "Some provisions of SH, for example the access provision, are easier to comply with compared to if the company had decided to abide by local laws or Model contracts. Also, from a company perspective, the rule on onward transfers is very interesting. In this regard, the SH does not stipulate how a potential contract should be drafted in order to transfer data from a SH entity to another controller established outside the EU. This means that once a company has transferred data to the US, it can transfer the data from there to everywhere in the world. Because there is no enforcement or surveillance, this is standard practice." "It provides the advantage of having a good reputation. It's a good marketing advantage (even if done for window dressing purposes)."

Lawyer C made reference to the "[r]elative ease of enforcing requirements, and the ability to keep EU DPAs out of the matter when non-employee data is subject to the SHA."

Lawyer D said: "In Spain, the main advantage of the SHA regime is that it is very easy to register a data transfer to the USA at the Spanish Data Protection Agency, unlike other transfers (for example based on the European Commission Standard Clauses)."

2) The **disadvantages** underlined are as follows: for lawyer A: "the major disadvantages are (1) localization of liability risks in the US, with the risk of large damage awards that

can bring, (2) the fact that SH only covers transfers to a single country, and (3) the fact that some important sectors (such as financial services and transportation) are excluded from it."

Lawyer B: "The SH places more burdens/obligations upon a company that uses it to legitimise transfers than if the same company uses consent as legal grounds. For example, if a company is able to obtain consent as legal ground for transferring data, from the company perspective, this is better because, generally speaking, the consent does not impose further obligations upon the company." "The fact that the company is under the jurisdiction of the FTC." "I find it to be a disadvantage that if a company wishes to use SH, this basically means that it will have to give SH treatment to all the data it receives from the EU (except for human resources data), (I realise that this may be an advantage as well). In contrast, if a company uses contracts, and, in the future it wants to use consent for other transfers, it still can do this. In sum, I find it to be a disadvantage that if a company subscribes to SH, then everything must be covered by SH."

Lawyer C pointed out the fact that the SHA is "[a]pplicable only to transfer from EEA to US."

Lawyer D added: "It is only valid for the transfers to the USA. If a corporate data transfer strategy requires data transfers to countries other than the USA, the European Union or countries that provide an adequate level of protection, the SHA regime only provides a partial solution, rather than a global one."

3) Regarding the question of whether the **EC Decisions on Model Contractual Clauses have any impact on the TBDF strategy**, lawyer A said: "Yes, certainly. The model contracts constitute another option for companies to provide a legal basis for transborder data transfers; I believe they are *per se* neither better nor worse than SH, since the decision to use a particular mechanism has to be determined based on the circumstances of each particular case. There are some cases for which SH is better suited (for instance, when a company in the US continually imports data from the EU), and others in which the model contracts may be more appropriate (e.g., when the importer is in a sector not covered by SH, or when the transfers are more limited in nature)."

Lawyer D added: "It is not feasible to seek global data protection compliance without taking into account the European regulations, and among others, the decisions on Model Contractual Clauses. Nevertheless, in some European Union member States (i.e. Spain), the European Standard Clauses are not as useful as they might seem, because they do not prevent a Spanish data exporter from having to seek prior authorisation for the transfer from the Spanish Data Protection Agency."

4) When asked if they think that **the SHA system results in a double data protection regime within companies (one of EU data and one of US data), or rather companies increase the US data protection regime to the SH regime or beyond it**, lawyer A said: "In my experience, what US companies want to avoid as much as possible is establishing multiple data protection regimes, since that creates substantial extra costs. Thus, they tend

to adopt the SH principles as the basis of their data processing around the world. I can think of several large US-based multinational companies that have joined SH and applied the SH principles to their data processing globally even outside the US (except for countries such as the EU where mandatory national data protection law applies, of course)."

Lawyer B considered that "Safer harbor leads to a triple data protection regime: the EU regime, the SH regime, and the regime for "US data" because I do not think companies provide SH rights to data gathered in the US."

Lawyer D pointed out: "I believe that companies that adhere to the SHA place their data protection regime in the USA at a similar level as that implemented in Europe."

5) Lawyers A and B said that companies normally conduct the **annual verification** internally, while lawyer C said that sometimes it is conducted internally and sometimes by a third party.

6) 7) None of them had any experience with **enforcement actions**, neither by **European DPAs**, nor by the **FTC**.

8) Lawyers answered that they follow their client's choice concerning **alternative dispute resolution bodies (ADRs)**.

9) None of them had any experience with **complaints before such ADRs**.

10) Concerning **the way access to data subjects is provided by the companies** they advise, lawyer A considered that "[t]his depends, of course, on which party has easiest access to the data—if the data is stored in Europe, then it is usually the exporter, and if it is in the US, the importer. In my experience, exporters and importers tend to work together in providing the most efficient mechanism for access.

Lawyer B said "[u]sually, via the data exporter because it's closer to the individual."

11) They have been also asked whether they believe that the SH regime offer a feasible **solution to conduct: -processor to processor transfers and -controller to processor transfers.** Lawyer A said: "[i]n my view, the SH documents are ambiguous as to whether they only cover controller-to-controller transfers, or whether other types of transfers are covered as well. Of course, the distinction between a controller and a processor can often be artificial, and it can often happen that a party's role changes from one transfer to another. I also think that there is no clear prohibition in SH to covering data transfers to processors. Thus, I believe that SH can cover transfers to processors as well. However, it would be useful if there was some clarification of this point in the documents."

Lawyer B said: "I think that it does. In particular, if you compare it with the Model contract where the question of transfers to processor simply is not contemplated (this is a big mistake), I find that the SH provides a feasible and proper rule."

12) None of their clients have experienced **limitations in the adherence to the SH principles** due to (a) necessity to meet national security, public interest, or law enforcement requirements (b) due to any statute, government regulation, or case law that create conflicting obligations or explicit authorizations

b) National DPAs

The questionnaire has been sent to the 18 EEA DPAs.

12 answers have been received so far. An overview of the answers per country can be seen in the grid incorporated in Appendix VII.

In general, it can be observed that since notification prior to transfers abroad is not required by all the DPAs, a full picture of the quantity and legal compliance of data transfers under the SH can not be obtained. The figures received from those DPAs that do require notification are not representative for two reasons: (1) only Belgium and Spain specified numbers of SH data streams, (2) these numbers are substantially lower than the total amount of companies that have self-certified. For instance, in Belgium 18 data flows under the SH have been declared since September 2001, of which 14 deal with human resources data. In Spain, 16 data flows under the SH have been declared. All those DPAs answered that the notifications they received were concerning intra-company or intra-group transfers.

Most of the DPAs have elaborated guidelines on TBDF with specific reference to the SH, or conduct other kind of pedagogical activities such as presentations to the business sector.

None of them treat differently those companies that have represented to cooperate with them *vis-à-vis* those who have not done so.

Any DPA has: (1) received complaints dealing with the SH, (2) received communications from the FTC to investigate, (3) approached the FTC to monitor and/or investigate compliance with the SHA, (4) suspended data flows under the SH, nor (5) initiated any informative procedure under Article 3.1.a) of the SH agreement.

The following remarks were added by the DPAs:

*Belgium: "[i]t seems that the SHA and the standard contractual clauses are not broadly used yet. SHA is mentioned in less than 10% of TBDF notified. The main legal basis for TBDF is consent and the fact that the TBDF is necessary for the performance of a contract. In more than half of the cases, several legal basis are used in order to secure the validity of a TBDF."

*Germany: "German companies tend to use the EU model clause or BDR for TBDF to the US rather than rely on the quite complex (and in respect of the categories of data non-concluding) SHA."

*Italy: "Reference may be made to some cases addressed by the Italian Garante, in which US-based companies appeared to prefer to avail themselves of standard contractual clauses (SCC) for transferring data to the US because they found that the SCC were more in line with EU data protection principles compared with the SHA. Additionally, the standard contractual clauses were considered to provide more clear-cut guidelines as to liability issues and implementing mechanisms."

*Portugal: "It is curious that controllers do not use SHA as a legal ground for TBDF to US, which would be easier to get a permit, but instead recourse to other instruments. We may say that SHA is far from being a successful solution in Portugal to TBDF to US."

*Spain: "In general, it must be mentioned that companies established in Spain rather like other systems (mainly the use of contractual clauses or asking for the consent of data subjects) than the SH approach for legitimating the transfers of personal data to the US. This is even more true since the approval by the European Commission of the Model Contractual Clauses. The most used argument in favour of this approach is the legal certainty provided by the other methods is greater than the ambiguous, complex and less than clear provisions of the SH Agreement."

c) FTC

So far, no answer to the questionnaire has been received.

d) Consumer Associations

The BEUC (Bureau Européen des Union de Consommateurs) has been contacted. They answered that they are not entitled to receive complaints, so they are not able to answer the questionnaire. They sent, however, position papers dated 1999, 2000, 2001 presented to the EC and to the press containing comments and analysis on the SH from a European consumer point of view. Furthermore, they recommended to contact their national members. As a consequence, a fax and e-mail has been sent to the members[71] (25 organizations) containing the questionnaire. So far, two answers have been received.

[71] The list of national members can be seen at: http://212.246.143/Content/Default.asp?PageID=184

The representative from Consumers' Association – CA (UK) said that after having checked their data base they can confirm that complaints have not been received. However, he said, "this is not an area in which we would necessarily expect to receive complaints.

The representative from National Consumer Council – NCC (UK) expressed that they are a policy organization and do not deal with complaints from consumers. She expressed that the organisation is publishing a book in autumn on consumer privacy.

e) DoC

When asked about a **description of the review procedure of the information contained in the Safe Harbour self-certification declarations** the representative form the DoC answered: "U.S. organizations may self-certify their adherence by submitting their self-certification materials on-line (via the Safe Harbor web-site at http://export.gov/safeharbor) or by sending a letter to the Department of Commerce. If the organization chooses to submit its materials on-line, it will electronically transmit two documents: 1) the organization=s self-certification form; and 2) a one-paragraph self-certification/affirmation statement from a company officer. If the organization chooses to send its self-certification materials through the mail, it must submit a cover letter from a company official along with its self-certification form. We receive between 10 and 30 self-certifications per month. Over 95% of self-certifications received have been submitted via the website."

"Upon receipt of an organization's self-certification materials, we review the submission in order to determine whether the organization should be placed on the Safe Harbor List. In making this decision, we will review the materials in order to determine: 1) Whether all of the required fields have been completed (Have the criteria specified in FAQ 6 been satisfied?); 2) If the organization's submission is responsive to the applicable fields on the form; and 3) If there are any inconsistencies on the face of the self-certification form (e.g. Does an organization list an inactive link as its privacy policy location?; Does the organization appear to fall outside the scope of Federal Trade Commission or Department of Transportation jurisdiction?)."

"An organization's self-certification to the Safe Harbor List, and its appearance on the list constitute a representation to the Department of Commerce and the public that it adheres to a privacy policy that meets the Safe Harbor framework. It is ultimately the responsibility of the organization to ensure that its privacy policy reflects compliance with the Safe Harbor. Therefore, we often advise organizations that, before self-certifying for Safe Harbor, they consider carefully the ramifications of the False Statements Act and the Federal Trade Commission Act."

"Organizations that decide to adhere to the Safe Harbor principles must comply with the principles in order to obtain and retain the benefits of the Safe Harbor and publicly declare that they do so. FAQ 6 requires Safe Harborites to state in their relevant privacy

policies that they adhere to the Safe Harbor principles. In addition, FAQ 6 requires Safe Harborites to provide a location where their privacy policy is available for viewing by the public. Organizations are often advised to state their adherence to Safe Harbor in their relevant privacy policies and/or to address each Safe Harbor principle and any applicable FAQ requirements within the text of the privacy policy."

"In addition, organizations should make their relevant privacy policies available to the general public. In certain cases, Internet-based privacy policies may satisfy this requirement. In other situations, including those where human resources data is covered in the self-certification, privacy policies housed on Intranet sites, in employee handbooks, or policies made available upon request (by contacting the organization) may satisfy the publicly available requirement."

"Our review of a self-certification normally takes one business day. If it is determined that an organization has submitted complete self-certification materials and that the materials are free of facial inconsistencies, an organization will be placed on the Safe Harbor List. There are currently 463 organizations on the Safe Harbor List. On average, between 10 and 20 organizations are added to the list each month."

"If it is determined that a submission is incomplete, an organization will be notified and asked to complete any applicable field. If any inconsistencies are visible on the face of the form, the organization will be contacted and asked to clarify its response(s). In some cases, we have refused to post organizations to the Safe Harbor List because incomplete or inconsistent areas of the organizations' self-certifications were not resolved."

"The organization's self-certification is valid for one year subsequent to the organization's placement on the Safe Harbor List. In order to continue to enjoy Safe Harbor benefits, an organization will need to reaffirm its self-certification on an annual basis. This can be accomplished by sending the Department of Commerce a letter or an e-mail that reaffirms its commitment to Safe Harbor. (Organizations may also submit a new self-certification form in order to complete its annual self-certification/reaffirmation requirement). Safe Harbor organizations receive periodic letters from the Department of Commerce advising the organization that its self-certification "Anniversary@ is approaching and that the Department of Commerce will require a letter from the organization reaffirming its Safe Harbor commitments. Organizations that have not reaffirmed their self-certification by their anniversary date are designated as "Not Current" on the Safe Harbor List and periodic e-mails are sent to the organizations to encourage their reaffirmation."

Concerning the **reception of any notification of company's persistent failure to comply with the Safe Harbor Agreement sent by any enforcement body (public or private)**, he said that they "have not received any notifications of an organization's "persistent failure to comply" status, nor are [they] aware of any such findings having been made by a self-regulatory program, the Federal Trade Commission, or the European Union Data Protection Authorities."

A description was also made about the **procedure followed when a company does not respect the annual verification**: "Under Safe Harbor Frequently Asked Question #7,

Safe Harbor organizations are required to retain their records on the implementation of their Safe Harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction."

"The Safe Harbor framework does not require the organization to submit its annual verification letter to the Department of Commerce and we are unaware of any failure of an organization to provide such a letter upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction."

"If we were to become aware of such facts indicating either that an organization has failed to complete its annual verification, or has failed to respond to a request in the context of an investigation about non-compliance, we would immediately contact the organization to determine the circumstances and if further action is warranted."

"In addition, under FAQ 11, if a relevant self-regulatory or government enforcement body finds an organization has engaged in a "persistent failure to comply" with the principles, the organization is no longer entitled to the benefits of the Safe Harbor. In this case, the organization must promptly notify the Department of Commerce of such facts either by email or letter. Failure to do so may be actionable under the False Statements Act. That organization must also provide the Department of Commerce with a copy of the decision letter from the relevant self-regulatory or government enforcement body. Self-regulatory or government enforcement bodies are also encouraged to notify the Department of Commerce of such facts."

Regarding **withdrawal of organizations from the SH list**, he answered: "Since the Safe Harbor's implementation, ten organizations have been removed from the Safe Harbor List at the request of the organizations. These withdrawals were mainly due to mergers or acquisitions or other cessation of the organizations' business and/or data collection activities." He added that "[they] do **maintain a record of organizations that have withdrawn** from the Safe Harbor List. A list of these organizations is available upon request. The Safe Harbor framework does not mandate that either the Federal Trade Commission or the DPA Panel be informed of such withdrawals as they occur. However, per Frequently Asked Question #6, organizations are required to notify the Department of Commerce. Withdrawal from the list terminates the organization's representation of adherence to the Safe Harbor, but this does not relieve the organization of its Safe Harbor obligations with respect to personal information received during the time the organization is on the Safe Harbor List." Furthermore: "The Safe Harbor framework does not require the Department of Commerce to maintain a separate list of organizations that withdraw from the Safe Harbor List on the Safe Harbor website. However, we do maintain a record of the organizations that have withdrawn. This record is available upon request."

f) ADRs

Considering that only one company answered to the questionnaire it is not possible to deduce conclusions. Furthermore, the said company pointed out that their US and EU complaints statistics are blended, so, it is not possible to identify the nature and details of the SH procedures.

3.5. Main findings

3.5.1. Positive trends

The analysis demonstrates that despite many shortcomings, some companies tend to invest in personal data protection. The following positive trends can be discerned:

- *Increased Participation vis-à-vis 2001 Intermediate Report.*

At the moment of the intermediate report only 48 US organizations signed up for the SH. As of 3 November 2003, 401 companies were mentioned in the DoC certification list. However, in order to be able to make an objective evaluation of this number it would be necessary to know how many US organizations import data from the EU.

- *Co-operation with DPAs.*

An important number of companies certified co-operation with the European DPAs. The analysis of the privacy policies indicates that certain companies accept to co-operate with the DPAs even though they do not process human resources data. Although the concrete motives could not be determined, and might for instance be laying in limiting legal uncertainty, it remains a positive observation.[72]

- *Additional Information in Privacy Policies.*

Some companies provide for information in their privacy policies which is not strictly required by the SH principles. For instance, an important number of companies that collect information online, give explanation about the use of cookies and log files.

- *Security Measure Compliance by Data Processors.*

US data processors generally represent to provide for security measures.

[72] Since there have been no enforcement cases by the DPA Panel so far, it is difficult to appraise the meaning of such declaration of co-operation. Neither is it entirely clear what the exact motives for co-operation.

- *Contact Information (in the Certification page).*

SH adherents provide full contact information in the DoC self-certification page. Privacy policies do, however, not always contain adequate contact information.

While certain companies were clearly not correctly implementing the SHA, non-compliance may be the result of lack of guidance and cultural differences. Certain companies clearly invest in a data protection regime, but may not be sufficiently acquainted with the concrete implementation of the principles in their daily business.

3.5.2.Neutral trends

- *The IT sector is the most represented industry sector within the US organizations that adhere to SH.*

- *Controller-to-Processor Applications*

9 of the reviewed privacy policies concerned controller-to-processor personal data transfers (2 of which import personal data also in a data controller capacity). The analysis of the certification page (sub. point 2.3.) demonstrates that 11% of the US organizations represented to import personal data as a data processor.[73]

The SH policies of these companies that are publicly available showed that in this case only the security principle has been implemented by the US organization. For instance, companies importing personal data as a data processor generally represent to provide for specific security requirements entailing authentication, authorization measures, audits, system security, disaster prevention and recovery, physical security measures and confidentiality guarantees.

Although the SH principles were not specifically designed to accommodate this type of personal data transfers, FAQ no. 10 "Article 17 Contracts" refers to this scenario. FAQ no. 10 recognizes that SH companies can participate to the SH framework but need to be further bound by a contract setting forth specific processing instructions, confidentiality requirements, and organizational and technical requirements as provided for in Article 17 of Directive 95/46/EC. US organizations that receive EU data for processing only, need not to implement the principles.

The SH principles were originally drafted for controller-to-controller data streams, and the text of FAQ 10 seems incompatible with the requirements set forth in the Commission Decision approving the model clauses for controller-to-processor transfers. It appears

[73] It must be noted that this number may vary depending on the statements made in the privacy policies.

that same level of protection should be guaranteed as in those clauses, and that an Article 17 contract does not suffice (see *infra*, contextual analysis).

- *Sensitive Data Transfers*

The number of companies that represent to transfer sensitive data under SH is limited (it concerns approximately one fifth of the reviewed policies). It must be noted that it concerns 8 companies, of which 6 have represented to transfer human resources data.

These numbers may not be generalized since an important number of policies that concern human resources data streams, and which typically contain a sensitive data, were not publicly available and thus were not reviewed.

- *In-house Verification*

An important majority of the companies have self-certified to provide for in-house verification methods. FAQ no. 7 sets forth specific quality requirements for self-assessments.[74] Furthermore, a statement verifying the self-assessment should be made available upon request by individuals. This obligation has not been evaluated.

- *Certification Status*

Most of the companies provided for a privacy policy that is current; 6% of the importing organizations did not have a current privacy policy. Non-currency does not imply absence of obligations. Even if a company cannot longer assume safe harbour benefits, it is still bound by made representations with respect to imported personal data: "The undertaking to adhere to Safe Harbor Principles is not time-limited in respect of data received during the period in which the organizations enjoys the benefits of the Safe Harbor. Its undertaking means that is will continue to apply the principles to such data for as long as the organizations stores, uses or discloses them, *even if subsequently leaves the Safe Harbor for any reason*."[75]

---

[74] FAQ no. 7 provides: "Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the safe harbour principles; that individuals are informed of any in-house arrangements for handling complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. [...] Organizations should retain the records on the implementation of their safe harbour privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction."

[75] Italics added.

- *No US regulatory or supervisory authority was selected apart from the FTC (except one that chose DoT).*

3.5.2. *Implementation Deficiencies Trends*

- *Corporate policies were often hard to find*

Locating the privacy policy may be difficult for various reasons. First of all, it may be difficult to locate privacy policies on the homepage. One can think that there is a practice consisting in putting the link at the bottom of the page. Nevertheless, this is not the case for a significant number of companies, they place it at the bottom of the web-page (left hand corner, center, right hand corner), at the top (left hand, center, right hand), or even in the center of the page, isolated or within a text. It must be observed that in some cases the link was not included in the homepage, requiring to scroll through the sitemap to discover its location. Apart from the place of the hyperlink, another fact that may render the localization difficult is the size of the characters which are sometimes too small. In addition, there is no uniform way to title privacy policies. The following titles were, for instance, given to privacy policies: Déclaration de protection des données, Legal, Legal Notice, Internet Policy, Privacy, Privacy Statement, Privacy Notice, Site Policies, Truste logo: EU-Site Privacy Statement, Legal Documents, Fair Information Privacy Statements, Terms of use, Use Policies, etc. A uniform typography and placement of (SH) privacy policy would help data subjects locating the

The following example shows a time-consuming search process data subjects have to go through to locate the policy: A company provides a direct link to a webpage named "About the [the Company's] WebSite Notice." On this page the company represents to abide to the SH principles, but the Notice does not provide further information. Individuals that are lucky enough to move with their mouse over a hidden icon that "SH" are directed to this company's SH page. The relation between the two web-pages is not clear, and consequently, it remains unsure whether certain statements made on the initial page ("About [the Company's] Website Notice") cover data transferred from the EU or not. The webpage titled "About [the Company's] Website Notice" provides a clause that seems to allude to onward transfers: "No matter what means you choose to communicate with [the Company], your E-mail and other personal information remain confidential. [the Company] do[es] not sell, rent, or give away such information to anyone, without a written permission obtained from the client and with the unique goal to develop the business interest of the client itself. [...]." The web-page that sets forth the SH principles does, however, under "onward transfer" not provide information whether personal information may be onward transferred and under what conditions: "Should [the Company] need the assistance of a commercial partner to develop the client's project, a co-finder agreement will be signed. It will cover all the aspects of privacy and security for the data received from the [the Company's] client and for their treatment."

Certain companies do not provide a direct link on the DOC certification page to their privacy policy. Other companies do not make their policies publicly available on the internet, but require data subjects to contact the relevant office to obtain a copy of the

policy. For instance, certain companies refer to their "Corporate headquarters," or mention that the organization can be contacted to obtain a copy of the privacy policy.

Another reason for making the identification the relevant privacy policy difficult is the fact that companies did not develop their own policy but adhere to the privacy policy of an organization to which they are member. For instance, certain research organizations are member of the "Council of American Survey Research Organizations ("CASRO")." A member's certification page provides for a direct link to a CASRO webpage that provides for a privacy policy. This privacy policy is, however, according to the SH standard, incomplete and its scope is not entirely clear (it sets forth guidelines for both individuals and "members"). The CASRO website contains a link to the CASRO Code of Standards and Ethics for Survey Research, which sets forth also certain privacy requirements. The Code does, however, not provide any reference in the title to "privacy," "data protection," "SH" or other relevant labels that could help determine data subjects that they are consulting the right web-page. In addition, the company that refers to the CASRO policy erroneously qualifies CASRO as a privacy program.

- *Self-certification despite non-existent or publicly unavailable policies*

One third of the companies under review did not have a policy which is publicly available on the internet. It mainly concerns companies that import human resources data and data processors. Other companies, do not offer a functional link on the certification website.

Although publication on the net is not required by the SH agreement, and the transfer of human resources generally only affects employees, it is difficult to see why an online publication is not made available.[76] Online publication would be of convenience for the direct availability to the DPA Panel in case it were necessary.[77]

- *Absence of publicly available privacy policy for certain data categories*

Certain companies certify for various data categories but only provide a link to a privacy policy for a particular data category, or publish a privacy policy that concerns data categories that are not covered by the certification letter. For instance, a company certified for "company, product, and/or service related information" and "human resources data." The link published on the DoC certification page does, however, lead to a privacy policy which concerns the collection and processing of personal information of [the Company's] website visitors: "By displaying the [privacy seal] mark, [the Company] has agreed to notify you of: What personally identifiable information or third-party personally identifiable information is collected from you through our website. [...]."

---

[76] Companies may argue not to do this because they do not want to render public their business strategies and other secret corporate information. Privacy policies must not contain such information, or would even not indirectly reveal such information.

[77] Commission Staff Working Paper of 13 February 2002 on the Application of Commission Decision 520/2000/EC of 26 July 2000: "[...] It would be preferable that even privacy policies only concerning employees be immediately and directly accessible by the relevant dispute resolution bodies (in this case the DPAs, as required by FAQ 9)."

Another Company self-certifies to cover "on-line, off-line, manually processed, and human resources data", while the privacy policy states: "All personal information obtained from users of the *site* will be handled in accordance with the terms and conditions of this Privacy Statement".

- *Style Differences and Lack of Clarity*

The reviewed privacy policies are marked by a difference of style. An important number of the reviewed policies require intensive reading to clearly understand what the US data importing organizations actually can do with the personal information. US organizations generally make efforts to describe how personal information is processed from a systemic point of view, but a clear description of data processing purposes has shown varying degrees of deficiencies over the entire line of policies that were assessed. Further, a distinction must be made between privacy policies that constitute also a notice, and privacy policies that do not. The first category, which is used by the majority of the companies, concerns privacy policies that translate and specify the SH principles into the corporate practice of the adherent. Such a policy will, for instance, specify the data processing purposes and explain how individuals can access their personal information. The second category retakes the SH principles without (consistently or clearly) indicating how the principles are implemented in practice. Such a policy will, for instance, provide for a representation that personal data will be processed for specified purposes and that individuals have right of access, but the purposes are not specified, and nor are the access modalities. In those cases, they have been awarded, nevertheless, a positive score for the various criteria, since they have made a representation, and if in the concrete case these companies do not comply with the made representations they would be in violation of the FTC Act.

The following deficiency typology can be recognized: (i) privacy policies are drafted in difficult language and a non-transparent manner; (ii) processing purposes are lacking, not clear, too broadly formulated, or mentioned at different parts within the policy; (iii) companies often use terms that are not clearly defined and that renders it difficult to understand and exactly estimate how somebody's personal information is used; and (iv) third party disclosure and choice is often non-transparent.

(i) privacy policies are drafted in difficult language and a non-transparent manner

Of approximately one third of the of the companies the notice was found to be lacking transparency. Privacy policies are often drafted in an eclectic manner, and data subjects may encounter difficulties to estimate data processing risks.

A limited number of privacy policies seem to be conceived as a contract. Certain policies provide for "disclaimer of warranties" and "limit of liability" or even set forth negative obligations (prohibitions) to individuals. For instance, a company that imports personal data in its capacity as a data processor sets forth the following security provisions: "Client is prohibited from violating, or attempting to violate, the security of the [Company's network]. Violations may result in criminal and civil liabilities to the Client. [The

Company] will investigate any alleged violations and will cooperate with law enforcement agencies if a criminal violation is suspected. Examples of violations of the security of the [Company's] network include, without limitation, the following: (i) Accessing data not intended for such Client; (ii) Logging into a server or account which the Client is not authorized to access; (iii) attempting to probe, scan or test the vulnerability of a system or network; (iv) breaching security or authentication measures without proper authorization; (v) attempting to interfere with service to any user, host, or network including, without limitation, by means of "overloading," "flooding," "mail-bombing," or "crashing," taking any action in order to obtain services to which the Client is not entitled." While these requirements may be inherent to the service agreement that this processor entity concluded with its Clients, one is wondering what security measures the data subject may account on if the data importer receives and processes personal data.

Another company describes it processing practices as follows: "Appropriate contact information for members may be given out to people requesting a referral for that profession. Referrals should be funnelled through the local Director. If the National Office has any reason to believe that the referral hasn't been followed up on, they may do so after seven days."

(ii) processing purposes are lacking or too broadly formulated

A recurrent problem with the assessed privacy policies was that data categories and processing purposes were "not sufficiently" defined. Approximately half of the reviewed companies does not or not clearly describe the purposes for which personal data is collected and processed. Not sufficiently means that individuals need to read the entire policy to have a sense about purposes and data categories, or worse, that it is impossible to clearly determine these elements.

The definition of the processing purposes is essential for data subjects to measure the risk of processing practices. Certain policies do not provide for processing purposes or describe it in cryptic language. For instance, a company provides that "personally identifiable information will only be collected to the extent that [the Company] deems reasonably necessary to serve a legitimate business purpose."

For instance, an organization indicates in its privacy policy the following relevant processing purpose: "[the Organization] collects limited personal data from different [Organization] regional offices and members worldwide in order to provide membership services to individuals." "Member Services" is further defined in the policy as follows: "[the Organization] uses personally identifiable information you have voluntarily provided on our Web sites, or by other means, to notify you via e-mail or printed material of [Organization] events or other relevant products and services offered by [the Organization]. Also, if you are a member of [the Organization] and/or part of an [Organization] specialty group or committee, [the Organization] will include your contact information in its directory of such members for networking purposes." The policy does not provide further clarification on the data processing purposes, and individuals only have some vague indication of this element.

Another company's data processing purposes are described as follows: "[the Company] collects your information in order to record and support your participation in the activities you select. The information that you provide is also used as part of our effort to keep you informed about product upgrades, special offers, and other products and services of [the Company]." While the second sentence indicates that personal data is used for direct marketing services, the first sentence is not clear.

Defining the purpose with a minimum degree of specificity is essential for data subjects to have a minimum idea of envisaged data processing. Additional guidance on this point is required.

(iii) use of unclear terms or incorrect definition

Privacy policies tend to use terminology that is not clearly defined. An example, is the varying conception of "personal information," "technical data," "demographic information," and "aggregate information." Data subjects may encounter difficulties clearly understanding how their data is processed as illustrated by the following example: "[the Company] reserves the right to provide aggregate to third parties for statistical analysis. Such data will not be linked to any particular individuals."

In other cases key notions are defined differently than in the Decision. For instance a policy sets forth the following definition of personal data: "any information or set of information that identifies or could be used by or on behalf of the company to identify an individual. Personal information does not include information that is encoded or anonymized, or publicly available information that has not been combined with non-public Personal Information." In another case, anonymous information was defined as "information, which alone may not identify you, and includes both demographic and product ownership information. Demographic information is information such as a product owner's age, income, city, state, ZIP code, area code, gender, purchase history, and so forth. Product ownership information is information about the specific products you own, such as the products' model numbers, serial numbers, places of purchase, and so forth."

The Decision provides on this point that "personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a US organization from the European Union, and recorded in any form. Certain companies tend to restrict the scope of application to "personally identifiable information," without giving any guidance to data subjects what this notion concretely means.

(iv) Lack of transparency regarding third party disclosure and choice

Privacy policies need often scrutiny, and more than one reading to have a sense how companies intend to re-use or disseminate personal data. One company provides for information which is unrelated to opt-in for data processing. It represents under

"Sensitive Information Principle: [the Company] signs three types of documents with the clients: (i) a letter of intent, with the object of the collaboration, (ii) a non-disclosure agreement, (iii) a non-circumvention agreement. The information considered sensitive or confidential needs to be written on papers reporting the declaration "sensitive" on the page. The sensitive information transmitted electronically needs to be encrypted. At this regard both the parties involved in the electronic transaction will establish specific procedures. The collected data are stored in office computers or on paper." The notion procedures is the only word that vaguely refers to choice, but no concrete representation is made as regards opt-in.

There may be different reasons for these style differences: US companies are not acquainted with the data protection principles and need to go through a learning process.

Second, it is inherent to the system of enforcement of the SH regime that companies remain in the grey zone with certain statements. Liability exposure is directly linked to explicitness and clarity of announced data protection practices. This is inherent to the enforcement model of the SH principles, but is not unavoidable. It were therefore advisable that the DOC, possibly in co-operation with the competent European authorities, publishes a set of guidelines on the drafting of SH privacy policies. The DOC could also publish a format that helps companies in their drafting process. Such guidelines could be developed in co-operation with the European DPAs, represented in the Article 29 Working Party.

- *Ambiguous and contradictory policies (or parts of policies were flawed by this deficiency)*

An important number of companies publish privacy policies containing contradictory statements. In most cases not the entire policy is suffering from this deficiency, but only certain parts. It must, however, be observed that the parts that lack transparency are often those parts that are essential to offering adequate protection to individuals. The problem is not the amount of information provided, but rather the quality of insight given to data subjects about the collection and processing of personal information pertaining to them.

Organizations may not make clear statements concerning dissemination practices. The following example it can be seen that it is not possible to determine what is the essential role of the said "partners," whether they are data controllers or data processors: "Our site provide users the opportunity to opt-out of receiving communications from us and our partners at the point where we request information about the visitor." In addition, this policy is patently contradictory where it also states that "we will not rent, sell, or disclose information to a third party."

Furthermore, companies' privacy policies use legal concepts that may be open to broad interpretation. For instance, a company sets forth that "[b]eyond its representatives and affiliates, [the Company] does not offer or allow the selling of any user-provided information to third parties." Although this provides some direction to individuals, it is not exactly clear what is meant with "representatives and affiliates." The policy further mentions on the next page that "[the Company] may occasionally present a special contest

or promotion that is sponsored by another company. To qualify for entry, we may ask you to provide personal information. If we plan to share that information with the sponsor(s), we will provide an up-front to that effect." No reference is made under this scenario to the individual's right to opt-out. It is not clear whether this company considers a sponsor as an "affiliate" or a "third party."

Another example, is a third party disclosure clause setting forth that "[the Company] will not share any of your individual information with third parties outside of *strategic partners* (contracted email delivery form, or affiliates which we deem helpful to our member's experience on the site) unless you have specifically requested for [the Company] to share your information with *select companies.*"[78] The paragraph dealing with "Limits of Confidentiality," only sheds limitedly some light on these concepts: "[the Company] may disclose personal information to special partners when it benefits our members. Special partners include companies that we have deemed to add value to our service and provide members with additional benefits. This type of partnership is rare, and is reserved only for those special partners that we have contracted with, who will provide additional benefit for our members. [...]." The extent of choice offered here, can only effectively be assessed if the meaning of "strategic partners" and "select companies" is clarified.

- *Incoherencies between certification pages and privacy policies*

Certain companies under review provide on the DOC certification page to process certain categories of personal data but the privacy policy to which the certification page refers covers other data types, or only one or certain data types of these announced on the certification page. For instance, a company certified to process both online and offline data, while the policy that was made publicly available only concerned the first category. Other companies certified to process both commercial and human resources data, but the policy only covered the collection of personal data via the company's website.

- *Incomprehensive description of data processing activities*

A considerable amount of privacy policies score insufficient as regard the description of their data processing practices, both in the certification letter as well as in the policy. Certain descriptions are too short and opaque and impart no or little meaning. Others provide for descriptions which are inappropriate. For instance: "[the Company] is the sole owner of the information collected on this site. We will not sell, share, or rent this information to others in ways different from what is disclosed in this statement. [The Company] collects information from our users at several different points on our website. With respect to any data transferred from the EU, [the Company] will hold such data for each customer securely and all data is the sole property of the customer. [The Company] will store and protect this data."

---

78 Italics added.

Certain data processing practices description are entirely irrelevant. An example is provided by the following description: "[the Company] is a leading provider of proprietary and patented reservoir description, production enhancement and reservoir management services. This services enable [the Company] clients to optimise reservoir performance and maximise hydrocarbon recovery from their producing fills. The Company has affiliates over 70 offices in more than 50 countries and its affiliates are located in every major oil-producing province in the world. The Company provides its services to the world's major national and independent oil companies."

- *False, misleading or irrelevant statements in their certification statements or policies.*

Some adherents certify to implement the SH requirements while the practice described with the matching principle is irrelevant.

For instance, one company translate the choice principle to its corporate practice as follows:

"[the Company] discusses the policy for personal/ technical treatment with the client itself; this claim is enclosed into the Agreement. The classic security triad referred to confidentiality, integrity, availability is applied to the received information. In particular,

- confidentiality implies control possession
- integrity implies authenticity and non-repudiation
- availability implies the utility of information"

The policy does not indicate whether data subjects effectively have a right to opt-out. The relevant parts of the policy dealing with sensitive data, onward transfer, and enforcement neither confirm whether individuals are effectively offered choice and the exercise modalities of such choice, if any.

Another examples concern enterprises that certify to adhere to a privacy program while this is not true.

Another company includes a clause of exclusion and limitation of liability: "**Damages**. In no event shall [the Company], its parent, subsidiaries, affiliated companies, agents, shareholders, employees or officers have any liability hereunder to you or any third party for any indirect, special, incidental or consequential damages (including damages for loss of business, loss of profits, litigation, or the like), whether based on breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages. In no event shall de aggregate liability of [the Company], its parent, subsidiaries, affiliated companies, agents, shareholders, employyes and officers exceed one hundred dollars ($100), regardless of the cause, whether in contract, tort, or otherwise. The foregoing limitations are fundamental elements of the basis of the bargain between [the Company] and you. This site and the materials would not be provided without such limitations."

The same company includes another contradictory clause: "**General.** This Policy constitutes the entire and only agreement between [the Company] and you regarding this subject matter and supersedes all prior or contemporaneous agreements, representations, warranties and understandings with respect thereto. You agree to review this Policy prior to reviewing any information or obtaining any documents from the Site. Any action related to this Policy shall be governed by the substantive laws of the State of California, without regard to conflicts of law principles. The State and Federal courts located in Santa Clara County, California, shall have sole jurisdiction over any dispute arising hereunder, and the parties hereby consent to the personal jurisdiction of such courts and to extra-territorial service of process. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Policy. Neither this Policy, nor any rights hereunder, may be assigned by operation of law or otherwise, in whole in part, by you without the prior, written consent of [the Company]. Any purported assignment without such permission shall be void. [The Company] may assign this Policy, in whole or in part, without notice to you. Any waiver of any rights of either party must be in writing, signed by the waiving party, and any such waiver shall not operate as a waiver of any future breach of this Policy. In the event any portion of this Policy is found to be illegal or unenforceable, such portion shall be severed, and the remaining terms shall be separately enforced. The language in this Policy shall be interpreted as to its fair meaning and not strictly for or against either party. This Policy may be modified or amended by you only in writing, signed by both parties. Any purported modification or amendment inconsistent with the foregoing shall be void."

"**Grant of Rights.** You represent and warrant that all information provided by you in whatever format shall be non-proprietary to you or any third party, and [the Company] may use or disclose such information without notice to, or permission from, you or any other third party, subject only to the Policy. You hereby grant to [the Company] a worldwide, royalty-free, irrevocable, perpetual, non-exclusive, transferable license (with a right to grant sublicenses through multiple tiers of sublicensees) to use, execute, display, copy, perform and modify such information as [the Company] sees fit for internal business purposes."

- *Certain companies only partly implement the principles*

The privacy policies of certain companies do not explicitly recognize all of the 7 SH principles.

1. Notice

    - Lack of clarity and conspicuousness
    - Lack of specified purposes (cf. *supra*)
    - Lack of organization contacts in the privacy policy
    - Lack of clarity for choice

The choice principle was generally found to be problematic. This is so, first because the purposes of the data processing are often lacking clarity (cf. *supra*). More than one third of the reviewed policies do even simply not provide for choice of dissemination of

personal data or provided it in an incomprehensible manner (*inter alia* because the notion of "third parties" is mostly not defined). A company's privacy policy provides in the paragraph entitled "Limits of Confidentiality" for the disclosure of personal information to "special partners" but does not set forth any possibility for the data subject to opt-out from such an envisaged transfer. The same company's privacy policy offers choice to data subjects as regards the communication of information to advertisers. This scenario is, however, different from the disclosure of information to "special partners," regulated elsewhere in the policy.

Some companies provide for a mechanism whereby the effectiveness of the opt-out system is limited. This mechanism exist in providing opt-out boxes that are pre-ticked to providing permission to onward transfer personal information. The online privacy policy of an adherent states the following: "Except as otherwise noted in this policy [the Company] only discloses user information in aggregate form to marketing partners. For example, we might tell a marketing partner how many users visited [the Company] over a period of time, but we will never tell them who it was that saw or clicked on their offer, unless that user has given us permission to do so. [The Company] believes that consumers should be able to control the use of their data. We will not share personally identifiable information with marketing partners if you follow the simple opt-out procedure of removing the check mark located at the permission notice box appearing on the [company] registration and entry page. [...]." This system does not comply with the opt-out requirement as described in the SH choice principle, pursuant to which onward transfer is the exception and not the rule.

- Lack of SH compliance statement

2. Choice

   - Not readily available
   - Lack of representations concerning affordability
   - Sensitive data (cf. *supra*)

3. Onward Transfer

   - Lack of third processors commitment to safe harbour

4. Security

   - Lack of security measures

5. Integrity

   - Unclarity of the relevance of data for specified purposes
   - Lack of representation to ensure reliability for intended use

6. Access

   - Lack of reasonable access

Approximately half of the reviewed policies did not provide for reasonable access, and none of the policies made a statement on the affordability of access. Approximately one third of the companies did not provide for a right to correct data, and approximately half of them provided for an opportunity to delete inaccurate data. With regard to online data collection and processing is the right of access often restricted to contact data only. This is so because the right of access is implemented by giving data subjects an opportunity to reset preferences in their personal account.

A recurrent failure is that although companies grant an opportunity to individuals to amend personal information, no explicit right of access is foreseen. For instance, a company provides in its Privacy Statement that "Users can amend this information [i.e. collected information from it's sites] through the web site on most [of Company's] sites, or if that feature is not available, by sending an e-mail to [questions@company.com]. This company does, however, not make a representation that individuals have a right of access independently of their wish to have personal information modified. As a general trend, the right to access seems problematic under the SHA.

- Absence of reference to cost
- Lack of correction, amendment or deletion

7. Enforcement

The enforcement principle is also problematic. [ ] organizations/companies represent to have enrolled into a privacy program, while the explanation they provide demonstrates that this is most likely not the case because they refer (i) to non-verifiable in-house measures the description of which has nothing to do with a real "privacy program; or (ii) to mere dispute resolution programs, which clearly do not fall under the denominator "privacy program."

- Limited number of companies agreed to accept reverse effect of breach, SH compliance of future processing, cessation, publicity of decisions
- Limited number of companies agreed to comply with the DPA advice
- Absence of sanctions

4. Contextual analysis of the SHA

4.1. Impact of new TBDF regimes (4.1.1. Model contractual clauses and 4.1.2. Binding Corporate Rules)

A general comparative analysis[79] of (i) the SH documents, (ii) the EU Decision on Model Contracts[80] -DMC- and (iii) the Article 29 Data Protection Working Party Working Document on Binding Corporate Rules[81] –WDBCR[82] leads to the following considerations:

First, the legal basis of these different data transfer mechanisms and documents is different. The SHA is based on Article 25(6) of Directive 95/46/EC, and thus constitutes an "adequacy finding". The other two documents are (or would be in the case of WDBCR) based on Article 25(2) of Directive 95/46/EC. Consequently they do not imply an adequacy finding, but an appropriate safeguard that allows to make a safe data transfer, not on an ongoing basis, as is the case of adequacy findings, but on a *case-per-case* basis.

Second, it appears that the main impact that later documents may have in the assessment of SH derives from the emphasis on "enforcement" procedures and obligations that is contained in those documents. Indeed, both the DMC and the WDBCR requires, for instance, the mandatory co-operation with the European DPAs and the jurisdiction of European courts (in the case of DMC this is optional for the data subject).

The Article 29 Working Party has pointed out: "[D]ata subjects should be entitled to enforce compliance with the rules both by lodging a complaint before the competent data protection authority and before the competent court on Community territory as explained later in section 5.6. The Article 29 Working Party gives great importance to the existence of both possibilities. Although it seems practical for data subjects to lodge a complaint with the competent DPA, and indeed the duty of co-operation of the corporate group with the authority is likely to solve most of the problems. A judicial remedy is, however, still required for the following reasons (see section 5.6): (a) the co-operation duty can not guarantee full compliance with the rules, and data subjects may not necessarily always agree with the views of the DPA; and (b) the competence of the DPAs in the Community may vary between the member states (e.g. some authorities may not impose sanctions or

---

79 To be completed. See table on Appendix VIII

80 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 1539), Official Journal L 181 , 04/07/2001 P. 0019 - 0031

81 Article 29 data Protection Working Party, Working Document: "Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers", WP 74, Adopted on 3 June 2003

82 For a deep study on the Working Document on Binding Corporate Rules see : Y. Poullet "Flux transfrontières des données, vie privé et groupes des entreprises. A propos d'une opinion récente du Groupe de travail de l'Article 29 sur la protection des données", Colloque de l'AEBDF, Monaco, octobre 2003.

block transfers directly) and none of them can award compensation for damages, only courts can do this.

Although the possibility for data subjects to enforce the rules before the courts is a necessary element for the reasons just mentioned, the Article 29 Working Party attaches more importance to the fact that the rules are complied with in practice by the corporate group as is the aim of any self-regulatory approach."[83]

Furthermore, audits conducted both internally as well as by external accredited auditors must be foreseen in the BCR. Such audits would be conducted on a regular basis and DPAs would receive a copy of the results. The BCR would also indicate the duty of co-operation and compliance with the advice of the DPAs.

We have to bear in mind that the document on BCRs is not mandatory but represents the on-going work conducted by national DPAs in what concerns TBDF, and reflects also new trends already adopted in the DMC.

Concerning substantial principles, the DMC follows the Working Document no. 12. The WDBCR do follow the same Working Documents in this regard and further specify that those principles may mean little for companies or employees with a data protection tradition different than in Europe. Therefore, it is suggested that BCRs develop data protection principles in detail.

Moreover, whereas SH requires notice and choice for onward transfers, the DMC and WDBCR sets forth stricter requirements. The WDBCR requires the signature of MC, and the DMC specifically requires: "Restrictions on onwards transfers: further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

(a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer or, in other cases, have been given the opportunity to object.
The minimum information to be provided to data subjects must contain in a language understandable to them:

-the purposes of the onward transfer,
-the identification of the data exporter established in the Community,
-the categories of further recipients of the data and the countries of destination, and
-an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of individuals; or

[83] See p. 11-12.

(b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer."[84]

From a practical perspective, the unlimited material and territorial scope of application makes the documents useful for certain data streams that are not exclusively directed to the US or that concerns activities that fall outside the SH.

4.2) Impact of new US legislation

Prevailing Laws that Conflict with SH Principles

Since the adoption of the SH, the United States has enacted several privacy laws and regulations that might enable subscribing organizations to disregard SH principles. According to the SH, if US law requires subscribing organizations to ignore SH principles, the protection of personal information transferred will still be deemed "adequate." The SH provides that:

> "Adherence to these Principles may be limited: .... by statute, government regulation, or case law that create conflicting obligations or explicit authorizations."

The scope of this 'escape clause' is confusing because there is no definition of "conflicting obligations or explicit authorizations."[85] Part B of Annex IV attempts to explain the meaning of the term "explicit authorization." The Annex notes that this exception to SH treatment would apply when US laws "affirmatively authorize the particular conduct by SH organizations" and that the exception "would not apply where the law is silent." However, the Annex also notes "specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorization to disclose the information without notice and consent)." In other words, this interpretative guidance seems to imply that exemptions from privacy protections that are contained in US law are tantamount to "explicit authorization."

As a general matter, this escape clause may be very broad. Typically, US privacy laws and regulations provide a minimum level of protection and, thereby authorize any non-prescribed conduct. Indeed, statutory obligations frequently contain specific exceptions for more permissive treatment of personal information such as affiliate sharing without

---

[84] Appendix 2 & 3.

[85] A prior report to the European Commission on the Safe Harbor has shown that the explanatory material in Annex IV, Part B is contradictory. See Report on US/EU Safe Harbor and the Financial Services Sector (Dec. 2000).

consent. According to the interpretive guidance in Annex IV, these exceptions must be considered an 'explicit authorization.'

Organizations relying on the escape clause must demonstrate that "non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization" while "indicating in their privacy policies where exceptions to the Principles permitted by [statute]... will apply on a regular basis." In addition, the exception provides that if US law allows, "organizations are expected to opt for the higher protection where possible." To the extent that US law prescribes a minimum level of protection, organizations could always opt for higher protection.

Only a small number of organizations that subscribe to the SH indicate the escape clause in their privacy policies. In general, such references are very vague such as

- *"[company] may disclose user information when we believe in good faith that the law requires disclosure,"*
- *"[company] may make information available to law enforcement personnel and agencies as required by law ... and may disclose such information if required by law or a judicial or governmental order or subpoena"*
- *"this privacy policy is subject in all respects to applicable legal and regulatory requirements and limitations that would dictate actions or policies different from those set forth herein."*

These references do not provide sufficient transparency for data subjects to determine the exceptions that are applied to the company's privacy statement and to the SH principles. When one company did provide a more explicit reference, there was still no citation to any particular statute and the reference was rather confused. This company prepares balloting packages and conducts voting for clients' officers and bylaws elections. The privacy statement indicates: "state laws vary with respect to public access and use of this voter registration information." This indication makes no sense. State laws governing public access to voter registration apply to public elections and are not relevant for private elections such as those for corporate officers. Securities regulation, however, might impose disclosure obligations for the identity of private election participants.

Since too few organizations make any reference in their privacy policies to overriding legislation or legal rules and none cite specific rules, this analysis will therefore identify potentially conflicting obligations arising from key new legal rules that have entered into force in the United States between the adoption of SH and the Study deadline of November 1, 2003.[86]

---

[86] The European Commission has previously undertaken an analysis of conflicting rules in effect as of December 2000 for the financial services sector even though this sector is not covered by the Safe Harbor. See Report on US/EU Safe Harbor and the Financial Services Sector (Dec. 2000). Similarly, the European Commission has decided that conflicts regarding airline passenger data arising from the Aviation and Transportation Security Act, Pub. L. 107-71 (Nov. 18, 2001) and corresponding regulations have been resolved. See Communication from the Commission to the Council and the Parliament of 16.12.2003, COM (2003) 826 final (Dec. 16, 2003)

As an initial observation, there do not appear to be many new examples in US law where the escape clause affects data transferred from the European Union under SH. The most significant issues revolve around the USA PATRIOT Act.[87] This statute, adopted shortly after the September 11th terrorist attacks, created new law enforcement powers and modified many provisions of existing law to assist law enforcement in the deterrence and punishment of terrorist acts. The Act gives US law enforcement agents greater powers to access personal information and engage in surveillance activities. This expanded law enforcement authority remains controversial in the United States and many of the Act's provisions are irrelevant for SH because most of the Act does not pertain to activities covered by SH. For example, Title III of the Act relates to financial services that are outside the scope of SH. Oddly, however, the Act does contain a provision directly relevant to human resources data. In that same context, a recent decision in connection with affiliate sharing and credit reporting[88] may have significant implications beyond the financial services sector with respect to data integrity and onward transfer for human resources information. In the area of sensitive data, the U.S. Department of Health and Human Services issued health privacy regulations in August 2002 to implement the Health Insurance Portability and Accountability Act.[89] These regulations replaced the health privacy rules issued at the end of the Clinton Administration in 2000. Lastly, in the context of telecommunications services, several new rules or decisions affect the use of transmission data and personal privacy that may have a tangential impact on data originating in the European Union.

- *Law Enforcement: USA PATRIOT Act*

The USA PATRIOT Act contains a number of provisions that override the SH principles of choice, data integrity and onward transfer.[90] Specifically, the Act authorizes, and in many cases, requires electronic communications service providers to disclose personal information to government agencies in connection with law enforcement investigations without affording any choice to the data subject. These disclosures typically relate to communications services such as transaction records or emails. For example, Section 203(a)(1) expressly authorizes the disclosure of grand jury information to a series of federal agents when the information relates to foreign intelligence or counterintelligence. Section 203(b) also allows the disclosure among law enforcement officials of the contents of electronic communications. The federal agents, however, may only use such information "as necessary in the conduct of that person's official duties." Section 210 expands the scope of information that may be obtained by a subpoena for records of electronic communications to include Internet connection information, payment information and information on types of services. Section 212(a)

---

http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/apis-communication/apis_en.pdf Analysis of those issues is, therefore, unnecessary and will not be re-visited in this study.

87 Pub. L. 107-56 (Oct. 26, 2001)

88 Bank of Am., N.A. v. City of Daly City, 279 F. Supp. 2d 1118 (ND Ca. 2003)

89 Pub. L. 104-191 (1996)

90 The analysis of the USA PATRIOT Act does not address provisions of the law affecting data privacy for activities not covered by Safe Harbor such as financial services, education records maintained by US education institutions, immigration eligibility or the monitoring of foreign students studying in the US.

expressly authorizes the disclosure by communications service providers of users' data to governmental entities when the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." Section 212(b) requires an electronic communications service provider to disclose basic information about subscribers to a governmental entity on the basis of an administrative subpoena.[91] Section 214 specifically authorizes the government to obtain a court order for the installation of pen registers and trap/trace devices to gather data within the United States for the investigation of foreigners. Section 216 gives the government the right to require through court order that electronic communications service providers install pen registers and trap/trace devices to capture transaction records of Internet users without notice to those users. Section 215 empowers the FBI to obtain a Foreign Intelligence Surveillance court order requiring the production of business records from organizations in the United States for foreign intelligence and international terrorism investigations. The court order is confidential and the party disclosing business records to the FBI is prohibited from revealing the existence of the order and record disclosure to the data subject. This power is very broad as the FBI need not identify the target of the investigation and can seek wide range of business records.

In essence, these provisions of the Act "expressly authorize" disclosures to a third party— government agencies— without the choice of the data subject for purposes outside the scope of those related to the original data collection. These derogations from the SH principles are nevertheless justified on law enforcement and security grounds. Indeed, a separate escape clause of the SH allows organizations to derogate from the SH principles "to the extent necessary to meet national security, public interest, or law enforcement requirements."

- *Human Resources Data: USA PATRIOT Act and Affiliate Sharing*

One of the miscellaneous provisions of the USA PATRIOT Act provides an express authorization for employers in the financial services sector to disclose negative suspicions about employees in written employment references. Section 355 authorizes, but does not require, federally insured banks and uninsured branches and agencies of foreign banks to disclose in written employment references "information concerning the possible involvement of such ... party in potentially unlawful activity."[92] This type of disclosure might contravene the data integrity provisions of SH because the Act provides no specific mechanism for an affected employee to challenge any inaccurate statements.

---

[91] The information is: name, address, local and long distance telephone connection records, or records of session times and durations, length of service, types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment. Section 212 also provides a more troubling authorization for service providers to disclose transaction records or other information relating to a subscriber or customer "to any person other than a governmental entity." This clause, however, is not an issue for Safe Harbor since the subscribers and customers will be US-based and the data in question will be of US origin.

[92] While financial services are excluded from Safe Harbor, this clause pertains to human resources data and is therefore relevant.

Similarly, the recent federal court decision in *Bank of Am., N.A. v. City of Daly City*[93] is likely to have an impact on human resources information. In a challenge to a state ordinance that required opt-in consent for financial institutions to share personal information among affiliates, the federal district court held that the federal Fair Credit Reporting Act pre-empted the stronger state law. The court found that the FCRA "expressly exempt[s] information shared among affiliates from the definition of a consumer report." As a result, the privacy protections of the FCRA expressly do not apply to data received by affiliates. Because the court's decision extended the affiliate-sharing clause to cover personal financial information in a context other than credit reporting, the decision means that the affiliate sharing exemption will apply to all areas covered by the FCRA. Since the FCRA expressly allows disclosure of personal information for employment purposes without consent,[94] the decision appears to allow the sharing of employment data among affiliates without limitation as to purpose and without consent. This apparent interpretation is contrary to SH principles and organizations are not likely to be able to show that non-compliance based on this statutory authorization is "necessary to meet the overriding legitimate interests furthered by such authorization."

- *Sensitive Data: HIPAA Regulations*

The initial regulations for health privacy were issued at the end of the Clinton Administration in December 2000. However, the Bush Administration modified the Clinton rules and promulgated new regulations on August 14, 2002 that took full effect on April 14, 2003.[95] The regulations protect "individually identifiable health information,"[96] though they exclude from protection health information maintained by an employer. Most of the HIPAA regulations will be inapplicable to EU data because they only regulate personal information held by "covered entities" such as US health care providers delivering services in the United States or health insurance plans. However, organizations that provide billing services or clearinghouse functions and that receive individually identifiable health information in the course of their processing are "covered entities."[97]

The HIPAA regulations authorize a "covered entity" to use and disclose personal information without the patient's consent for "treatment, payment ... health care operations .... public interest and benefit"[98] These exceptions from consent may conflict with choice requirements in the SH for sensitive data. Significantly, the regulations also exempt certain marketing activities from patient consent.[99] This explicit authorization for the use of sensitive data is in conflict with SH principles of choice and data integrity.

---

93 279 F. Supp. 2d 1118 (ND Ca. 2003)

94 15 U.S.C. § 1681b(a)(3)(C)

95 See 45 C.F.R. Parts 160 and 164. See also Dept. of Health and Human Services, General Overview of Standards for Individually Identified Health Information (Dec. 2, 2002, as revised Apr. 3, 2003) http://www.hhs.gov/ocr/privacysummary.pdf

96 45 C.F.R. § 160.103.

97 45 C.F.R. § 160.103; 45 C.F.R. § 164.500(b)

98 45 C.F.R. § 164.502(a)(1)(ii)

99 45 C.F.R. § 165.514(e)(1)

- *Telecommunications data*

Several recent decisions may have an adverse effect on the SH principles of choice and integrity. In the context of choice, personal information of Internet users and telecommunications customers may now in certain circumstances be disclosed without the consent of data subjects for purposes that are outside those associated with the collection of the personal information. In particular, the identity of Internet users may be revealed to third parties without the consent of the Internet user. A number of court decisions under state law allow parties in a civil law suit to obtain a court order compelling the disclosure by Internet service providers of the identity of Internet users or anonymous posters on bulletin boards when those users are alleged to have engaged in illicit conduct.[100] Such derogation from the SH principles would, however, be justified as necessary to meet an overriding legitimate interest.

For telecommunications data, the Federal Communications Commission issued new regulations on "customer proprietary network information" in July 2002.[101]

These rules followed an adverse court ruling against the previous opt-in regime.[102] The new regulations allow communications companies to use CPNI of subscribers without subscriber consent for marketing services in the same category[103] and with notice and opt-out for a variety of other uses as well as opt-in for certain specific cases.[104] While subscriber information will not be of European origin, these regulations have the odd effect of authorizing the use of third party data that might be of European origin without any protections. Third party data will be contained in subscriber CPNI such as calling patterns between the subscriber and third parties. Yet, the regulations do not require any confidentiality with respect to the non-subscriber information. As such, the permissive use of non-subscriber data deviates from SH principles.

Most recently, the implementation by the Federal Trade Commission and the Federal Communications Commission of the National Do-Not-Call list for telemarketing[105] has the unintended consequence of authorizing outbound telemarketing to European phone lists and effectively exempts this use from the consent of those European subscribers. Telemarketers are permitted to make commercial solicitations to phone numbers as long as they have assured that the numbers are not registered on the national do-not-call list

---

100 See e.g. Immunomedics, Inc. v. Jean Doe, 775 A.2d 773 (N.J. Super. 2001)(compelling ISP to disclose the identity of an anonymous poster who was alleged to have violated an employment agreement.) See also John Doe v. 2TheMart.com Inc., 140 F.Supp.2d 1088 (W.D. Wash. 2001) (establishing a four part test to determine when the identification of an anonymous writer may be compelled)

101 In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96- 115, THIRD REPORT AND ORDER AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING Adopted: July 16, 2002 Released: July 25, 2002 http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-214A1.pdf, codified at 47 C.F.R. Part 64

102 U.S. West v. FCC, 182 F.3d 1224 (10th Cir., 2000)

103 47 C.F.R. § 64.2005(a)

104 47 C.F.R. § 64.2007

105 See Do-Not-Call Implementation Act, Pub. L. No. 108-10, 117 Stat. 557 (2003); 16 C.F.R. § 310.4(b)(1)(iii)(B) (FTC rule); 47 C.F.R. § 64.1200(c)(2) (FCC rule); Mainstream Marketing Services, Inc. v. Federal Trade Commission, 2004 U.S. App. LEXIS 2564, (Feb. 17, 2004)(upholding the legality of the Do-Not-Call list against a Constitutional challenge).

maintained by the Federal Trade Commission.[106] Registration on the do-no-call list is voluntary and, 55 million US telephone numbers were registered during its first six months of operation.[107] However, non-US telephone numbers are not eligible for registration. Consequently, telemarketers are expressly authorized to use any European telephone lists for telemarketing without the consent any European telephone subscribers. While this would deviate from the SH principles of choice and, possibly data integrity, the transfer of European telephone lists under SH to US call centers for telemarketing is likely to be a rare occurrence.

[106] 16 C.F.R.§ 310.4(b)(3)
[107] See FTC, Press Release: Compliance with Do Not Call Registry Exceptional (Feb. 13, 2004) http://www.ftc.gov/opa/2004/02/dncstats0204.htm

IV. Conclusions

The SH implementation review indicates that although US organizations that participating to SH do efforts to accommodate privacy concerns of EU individuals, important improvement is required to ensure that personal data streams under the SH are effectively adequate. As a general observation, the majority of the reviewed US organizations seem to have difficulties to correctly translate the SH principles in their daily data processing practices. Implementation deficiencies are not necessarily the result of bad faith but likely find their origin in a different perception of personal data protection at the other side of the Ocean. These problems can be overcome by providing more and better guidance on the mechanics as well as the meaning that the SH data protection principles have in the European legal tradition.

SH participants generally scored well as regards formal requirements that need to be fulfilled in the certification process. The positive tendencies, as described in the report, are minimal but nevertheless not unimportant. They demonstrate that US organizations are sensitive for the data protection issue and are willing to invest. It may, in this regard, not be forgotten that a thorough understanding of this matter has also taken time in Europe and is a continuous ongoing process. From a legal point of view this does not suffice and the following most important deficiencies are alarming:

- Lack of transparency of notices or privacy policies: privacy policies were generally difficult to read and were often not able to provide transparent insight of data processing activities and associated risks.

- Choice was unclearly mentioned, or lacking. Choice is crucial for data subjects to have minimal control as regards the processing of personal data pertaining to them. Without effective choice personal data can be imported, used and distributed without any restriction. Representations as regards the affordability of choice was generally missing.

- Inadequate formulation of data processing purposes. This makes it difficult, if not impossible, to appraise whether personal data collection and processing modalities are legitimate and/or relevant.

- Access. The right of access shows to be often limited to contact information, or is not offered. Further representations as regards the affordability of access are generally missing.

- Enforcement deficiencies. Organizations accept to co-operate with the DPA Panel (even if they do not process human resources data), but generally do not represent their acceptance to comply with the DPA Panel's advice. Organizations represent to adhere to privacy programs, which are no privacy programs. Certain dispute resolution bodies/programs that are used lack data protection expertise and adequate sanctioning mechanisms.

The answers of the DPAs demonstrates a low awareness of data subjects since no complaints/claims have been received and treated with respect to SH. Given the results of the review this can not be explained by compliance perfection, but by the lack of awareness with data subjects. For instance, the fact that privacy policies are generally drafted only in English does not enhance awareness.

It is believed that improved implementation of the SH principles could be attained via better guidance and education:

- It were advisable that the DoC publishes a set of guidelines on the drafting of SH privacy policies. The DoC could also publish a format that helps companies in their drafting process. Such guidelines could be developed in co-operation with the European DPAs, represented in the Article 29 Working Party. Additional guidance is required as regards the characteristics and function of "privacy programs" and "dispute resolution mechanisms."

- While the assessment of the legitimacy of data transfers under the SH principles falls outside the scope of this study, it is considered appropriate to indicate that the DoC certification page requires companies to select whether they are importing personal information in their capacity as a data processor or as a data controller (or both). In this context, further guidance as to the requirements US data processors need to comply with would be helpful.

- Clear guidance as regard the jurisdiction of the FTC is required as regards human resources and other personal data streams where the jurisdiction of the FTC is doubtful.

- Privacy policies, as well as websites of official SH authorities, such as the DoC, FTC, DPAs, the European Commission's relevant Data Protection website, should provide for a link to the DPA Panel website. The complaint procedure to the DPA Panel should be more transparent and be translated to all EEA countries language.

- Privacy program service providers and dispute resolution service providers should be subject to minimum quality standards as regards data protection expertise, available sanctioning mechanisms, responsiveness, etc.

APPENDIX I

Analytical Criteria for SH Adherents

1. *Eligibility Criteria*

The first category "Eligibility" identifies elements in the SH and FAQs that seek to establish whether a company's statements demonstrate that the company is, in fact, qualified to participate in SH.

- *The following elements provide a preliminary indication that an organization is eligible to benefit from the advantages of SH. The results of the analysis of these elements are included in Table 1.1 of Appendix III*

Public Disclosure of Privacy Policy[108] *(Yes/No)*

Commission Decision 2000/520/EC requires that the organization make a public disclosure of its privacy policy. Indeed, for the FTC to have jurisdiction over an organization under Section 5 of the FTC Act for engaging in an 'unfair or deceptive practice,' the organization must make a public statement of its policy.

Printable Policy (Yes/No)

As a practical matter, when an organization makes its public disclosure on the Internet, the policy must be printable so that data subjects, data exporters and data protection authorities can evaluate the privacy policy at a specific moment in time. If the policy is not capable of being printed, then there is no way to verify the terms of the policy applicable to data of European origin at any later point in time. This element indicates whether or not the policy can be printed.

Jurisdiction (FTC/DOT)[109]

SH requires that an organization be subject to the jurisdiction of either the FTC or the Department of Transportation. This element identifies the relevant jurisdiction.

---

108 Recital 5; Art. 2(a).
109 *SH Art. 1(2)(b).*

Coverage (Full/Limited)

Organizations may subscribe to the SH for the treatment of all their EU-origin data or for only some of their EU-origin data. This element seeks to identify the choices that organizations have made.

Policy Applies to EU Data Indefinitely (Yes/No)

FAQ 6 states that "the undertaking to adhere to the SH Principles is not time-limited .... [the] undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves SH." This element confirms whether organizations have made the commitment to apply their privacy polices to EU data for as long as the organization processes such data.

Policy Signals US Law Preventing Compliance (Yes/No)

The SH allows US law to override provisions of the SH if there is an explicit conflict between the two. This element identifies whether the organization has indicated any such conflicts.

- *SH also requires that the self-certification letter of each adhering organization contain particular information. The elements of this procedural eligibility are found in FAQ 6. The results of the analysis for these elements are included in Tables 1.2 and 1.3 of Appendix III.*

Name of Organizational Contact (Yes/No)
Address of Organization (Yes/No)
Telephone number (Yes/No)
Fax number (Yes/No)
Email[110] *(Yes/No)*
Description of the Types of Processed EU Data[111] *(Yes/No)*
Public Location of the Privacy Policy (Yes/No)
Accurate Location of the Privacy Policy[112] *(Yes/No)*
Date of SH Self-Certification[113] *(date)*
Effective date of privacy policy (date)
Organization's Contact Office (Yes/No)
Identification of the Regulatory Agency that may hear claims[114] *(Yes/No)*

---

110 This criterion indicates if the Certification lists either a general organizational email address or a specific contact email address for SH issues.

111 FAQ 6 requires that the certification include a "description of the activities of the organization with respect to personal information received from the EU."

112 This indicates if the address shown on the Certification is an accurate and precise location for the privacy policy. When the Certification indicates a web site that is not the actual page for the privacy policy, the location will be marked as inaccurate.

113 Although this is not precisely stated in FAQ 6, this element indicates when SH adherence takes effect.

114 FAQ 6 requires that the organization state the specific statutory body that has jurisdiction to hear claims against the organization.

Identification of the organization's membership in any privacy programs[115] *(name of program)*
Verification Method of Organizational Compliance (Self/Third-Party)
Independent Recourse Mechanism[116] *(DPA/name of other)*
HR Data + DPA Enforcement[117] *(Yes/No)*

2. Substantive Compliance Criteria

The second category "Compliance" identifies the elements of corporate privacy policies that show whether adhering organizations meet the substantive content requirements of the SH and FAQs. The Compliance criteria are divided into groups reflecting each of the SH principles (notice, choice, onward transfer, security, integrity, and access).

2.1 For the notice principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.1 of Appendix III.

Clear language (Yes/No)

SH provides that "notice must be provided in clear and conspicuous language." Clarity relates to the ease with which a data subject can understand the privacy policy. This element identifies whether the corporate policies are clear to an informed reader.

Conspicuous Language (Yes/No)

SH provides that "notice must be provided in clear and conspicuous language." Conspicuous means that the notice is readily found. The certification of an inaccurate location, for example, would be an illustration of inconspicuous notice. This element identifies whether corporate policies are conspicuously posted.

Specified Purpose (Yes/No)

SH requires that corporate policies notify data subjects of the purposes for the data processing. This element identifies whether corporate privacy policies contain purpose specifications.

Organization Contacts (Yes/No)

---

115 FAQ 6 requires organizations to state the name of any privacy programs to which the organization belongs.

116 FAQ 6 requires organizations to state the independent recourse mechanism that is available to investigate unresolved complaints.

117 FAQ 6 requires organizations processing human resources data to declare their commitment to cooperate with the DPA and to comply with the advice of such authority.

SH requires that privacy policies provide contact information for the corporation. This element identifies whether corporate policies include contact information.

Third Party Disclosures (Yes/No)

SH requires adherents to disclose if they transfer personal information to third parties. This element identifies whether corporate policies disclose third party disclosures.

Notice of Choice for use/dissemination (Yes/No)

The SH Notice Principle requires that data subjects be informed of their choices and the means to limit use and disclosure of personal information. This element identifies whether the corporate policies provide such notice.

Statement of SH Compliance (Yes/No)

FAQ 6 requires that "all organizations that self-certify for the SH must also state in their relevant published privacy policy statements that they adhere to the SH." This element identifies whether the corporate privacy policies make such affirmations.

2.2 For the Choice Principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.2 of Appendix III.

Opt-out (3rd party) (Yes/No)

SH requires an opt-out for the dissemination of personal data to third parties, other than those performing data processing services for the SH adherent. This element identifies whether corporate policies include an opt-out.

Opt-out (secondary use) (Yes/No)

SH requires an opt-out for the secondary use of personal data. This element identifies whether the corporate privacy policies include such an opt-out.

Clear language (Yes/No)

The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."

Readily Available (Yes/No)

The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice." This element identifies whether the corporate privacy policies provide a "readily available" mechanism to exercise choice. For this element, "readily available" will mean that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out) and that the opt-out mechanism be transparent for data subjects.

Affordable (Yes/No)

SH requires that the means to exercise choice be affordable for data subjects. This element identifies whether the corporate privacy policies indicate affordable means to exercise choice.

Opt-in (Sensitive Data) (Yes/No)

SH requires opt-in for data subjects. This element identifies whether the corporate privacy policy offers an opt-in for sensitive data.

2.3 For the Onward Transfer principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.3 of Appendix III.

Notice of Onward Transfers (Yes/No)

The SH provides that "to disclose information to a third party, organizations must first apply the Notice and Choice Principles." This element identifies whether company privacy policies provide notice of onward transfers.

Choice (Yes/No)

The SH provides that "to disclose information to a third party, organizations must first apply the Notice and Choice Principles." This element identifies whether the company privacy policies offer choice with respect to onward transfers.

3rd Party Processor's Commitment to SH (Yes/No)

SH requires that an organization may transfer personal data to third-party processors only if "the third-party subscribes to the Principles ... or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles." This element identifies whether the corporate policies indicate that any third-party processors have made commitments either to SH or to a contract with at least the same level of protection.

2.4 For the Security principles, the single element found in SH will be included in Table 2.4 of Appendix III

Reasonable Security Precautions (Yes/No)

SH requires that organizations take "reasonable precautions to protect [data] from loss, misuse and unauthorized access, disclosure, alteration and destruction." This element identifies whether the corporate privacy policies indicate reasonable security precautions.

2.5 For the Integrity principles, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.4 of Appendix III.

Relevance of Data for Specified Purpose (Yes/No)

SH requires that "personal information must be relevant for the purposes for which it is to be used." This element identifies whether the corporate policies indicate in some way that the data is relevant for the specified purpose.

Compatible/Authorized Processing for secondary use (Yes/No)

SH provides that "an organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual." This element indicates whether the corporate privacy policy makes a commitment to finality and either opt-in or opt-out for secondary use.

Steps to Ensure Reliability for intended use (Yes/No)

SH requires that "an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current." This element identifies whether the corporate privacy policies make any assertions regarding their steps to assure the reliability of their data.

2.6 For the Access principle, the following elements are found in SH and the results of the analysis for these elements will be included in Table 2.5 of Appendix III.

Reasonable Access Provided (Yes/No)

The SH requires that individuals "have access to personal information about them that an organization holds ... except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy." FAQ 8 notes that "if information is used for decisions that will significantly affect the individual ... then ... the organization would have to disclose that information even if it is relatively difficult or expensive to provide." FAQ 8 also states that "it is not

necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information." This element identifies whether corporate privacy policies make the commitment to provide reasonable access for data subjects to stored personal information that is not publicly available to the public at large and not combined with non-publicly available information.

Reasonable Cost for Access (Yes/No)

FAQ 9 permits organizations to "charge a reasonable fee" for access. This element identifies whether the organization indicates that it charges a reasonable fee. If the organization indicates that there is no fee for access, then the organization will also satisfy this element.

Correction / Amendment of inaccurate data (Yes/No)

The SH stipulates that "individuals must ... be able to correct, amend or delete information where it is inaccurate, except ... where the legitimate rights of persons other than the individual would be violated." This element identifies whether the organization states that data subjects may have inaccurate data corrected or amended.

Deletion of inaccurate data (Yes/No)

The SH stipulates that "individuals must ... be able to correct, amend or delete information where it is inaccurate, except ... where the legitimate rights of persons other than the individual would be violated." This element identifies whether the organization states that data subjects may have inaccurate data deleted.

3. Enforcement Criteria

The third category "Enforcement" identifies the elements satisfying the enforcement requirements of the SH with specific attention to FAQs 5 and 11.

3.1 The following elements provide an indication of the type of recourse mechanism chosen by the organization and the existence of remedies and sanctions. The results of the analysis for these elements are included in Table 3.1 of Appendix III.

Independent Recourse Mechanisms pursuant to FAQ 5 (Yes/No)

SH requires "readily available and affordable independent recourse mechanisms." This may be satisfied either pursuant to FAQ 5 or FAQ 11. This element indicates whether the organization has stated its intent to satisfy the independent recourse requirement pursuant to FAQ5.

Independent Recourse Mechanisms pursuant to FAQ 11 (Yes/No)

SH requires "readily available and affordable independent recourse mechanisms." This may be satisfied either pursuant to FAQ 5 or FAQ 11. This element indicates whether the organization has stated its intent to satisfy the independent recourse requirement pursuant to FAQ 11.

Obligation to remedy problem (Yes/No)

SH states that enforcement must include "obligations to remedy problems arising out of failure to comply with the Principles." This element identifies whether the organizational policy requires the organization to provide a remedy for non-compliance. If an organization belongs to a privacy program that requires its members to provide a remedy, then this element will be satisfied.

Sanctions for Violations (Yes/No)

SH requires that "sanctions must be sufficiently rigorous to ensure compliance by organizations." Any company that has elected DPA as a recourse mechanism, but that does not fully satisfy FAQ 5, cannot satisfy the sanctions requirement.

3.2 For organizations that have chosen independent recourse pursuant to FAQ 5, the following elements indicate compliance with FAQ 5. The results of the analysis of these elements will be included in Table 3.2 of Appendix III.

Elects enforcement by the relevant Data Protection Authority (Yes/No)

FAQ 5 requires that the organization declare in its self-certification that it "elects to satisfy [the recourse obligation] .... by committing to cooperate with the DPAs." This element identifies whether the organization has made this requisite statement. [this obligation must be fulfilled in the privacy policy. If a company has stated in its certification letter to elect DPA enforcement, but does not make such a statement in the privacy policy, then this requirement is considered not fulfilled].

Agrees to co-operates with Data Protection Authority (Yes/No)

FAQ 5 requires that the organization declare in its self-certification that it "will cooperate with the DPAs in the investigation and resolution of complaints." This element identifies whether the organization has made this requisite statement.

Agrees to comply with the advice of the DPA (Yes/No)

FAQ 5 requires that the organization declare in its self-certification that it "will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take remedial or compensatory measures." This element identifies whether the organization has made this requisite statement.

3.3 For organizations that have chosen independent recourse pursuant to FAQ 11, the following elements indicate compliance with FAQ 11. The results of the analysis of these elements will be included in Table 3.3 of Appendix III.

US Legal or Regulatory Supervision (Yes/No)

FAQ 11 allows the Enforcement Principle to be satisfied by "compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution." According to FAQ 11, this is in addition to any possible FTC recourse. This element identifies whether the organization has reported that it is subject to such US supervisory authority.

Independence of recourse mechanism (Yes/No)

FAQ 11 states that "Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record." Under FAQ 11, a company may satisfy this requirement by making a commitment to cooperate with the DPA or by submitting to an independent dispute settlement mechanism. This element identifies whether the organization has stated its submission either to the DPAs or to an independent dispute settlement mechanism.

Readily available/affordable recourse (Yes/No)

FAQ 11 states, "as required by the enforcement principle, the recourse available to individuals must be readily available and affordable." This element identifies whether the organization has stated recourse that appears readily available and affordable.

Transparency of dispute resolution procedures (Yes/No)

FAQ 11 requires that "recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works." This element identifies whether an organization has made the recourse mechanism transparent. If a company has elected DPA dispute settlement and indicates such mechanism in its privacy policy, then the process will be considered transparent. Similarly, if an organization has elected another independent dispute settlement mechanism, indicates such mechanism in its policy, and the mechanism's

procedures are available either through the organization or through the mechanism itself, then the recourse will be considered transparent.

Company agrees to reverse effects of breach (Yes/No)

FAQ 11 requires that the dispute resolution proceeding remedy result in a reversal of the effects of non-compliance. This element identifies whether the organization commits to reversing the effects of non-compliance with the organization's policy.

SH Compliant Future Processing (Yes/No)

FAQ 11 requires that the dispute resolution proceeding remedy result in future processing that will be in conformity with the SH Principles. This element identifies whether the organization commits to this remedy.

Cessation of processing of data for harmed individual (Yes/No)

FAQ 11 requires that the dispute resolution proceeding remedy result in the cessation, when appropriate, of or processing the personal data of the individual who brought the complaint. This element identifies whether the organization commits to this remedy.

Publicity for Findings (Yes/No)

FAQ 11 states that "sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances." This element identifies whether the independent dispute settlement mechanism elected by the organization is required to provide publicity for all findings of non-compliance.

Sanctions (Yes/No)

FAQ 11 requires sanctions that "could include suspension and removal of a seal, compensation for individuals for losses ... and injunctive orders." These sanctions must be in addition to any possible FTC action. Also, FAQ 11 requires that sanctions include "the requirement to delete data in certain circumstances" depending on the dispute resolution body's interpretation of the data's sensitivity. This element identifies whether an organization appears to be subject to such sanctions. Any company that has elected enforcement by a DPA, but has not agreed to abide by the DPA decision does not qualify for sanctions. Any organization that belongs to a privacy program whose rules provide for the removal of a seal in the event of non-compliance does qualify.

3.4 For organizations that rely on an independent dispute settlement mechanism, the following elements indicate whether the independent dispute settlement

mechanism complies with FAQ 11. The results of the analysis of these elements will be included in Table F of Appendix III.

Investigation of each complaint (Yes/No)

FAQ 11 states that "Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous." This element identifies if the dispute resolution body states that it investigates each complaint.

Readily available/ Affordable Recourse (Yes/No)

FAQ 11 provides that "as required by the enforcement principle, the recourse available to individuals must be readily available and affordable." This element identifies if the recourse appears to be readily available and affordable.

Transparency of Recourse Procedures (Yes/No)

FAQ 11 states that "recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices." This element identifies whether the independent recourse mechanism provides information on the procedures for filing a complaint and dispute settlement.

DRB Obtains Reversal of Effects of Breach (Yes/No)

FAQ 11 states that "the result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization." This element identifies whether the independent dispute resolution body appears to have the authority to obtain the reversal of the effects of non-compliance.

DRB Obtains SH Compliant Future Processing (Yes/No)

FAQ 11 states that "the result of any remedies provided by the dispute resolution body should be ... that future processing by the organization will be in conformity with the Principles." This element identifies whether independent dispute resolution body appears to have the authority to compel that future processing by compliant with SH.

DRB Obtains Cessation of Processing (Yes/No)

FAQ 11 states that "the result of any remedies provided by the dispute resolution body should be ... where appropriate, that processing of the

personal data of the individual who has brought the complaint will cease." This element identifies whether the independent dispute resolution body appears to have the authority to order the cessation of processing.

Compensation for Harm (Yes/No)

FAQ 11 provides that "sanctions could include ... compensation for individuals for losses incurred as a result of non-compliance." This element identifies whether independent dispute resolution bodies appear to have the authority to order such compensation.

Privacy Program Sanctions (Yes/No)

FAQ 11 provides that "sanctions could include suspension and removal of a seal." This element identifies whether privacy program rules require the suspension or removal of the seal from organizations not in compliance with the program's privacy principles.

Publication of dispute resolution body's sanction (Yes/No)

FAQ 11 requires that "sanctions should include publicity for findings of non-compliance" by the independent dispute resolution mechanism. This element indicates whether the dispute resolution body publicizes all findings of non-compliance.

Mandatory Referral of dispute resolution body's sanctions (Yes/No)

FAQ 11 states that the "private sector dispute resolution bodies and self-regulatory bodies must notify failures of SH organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts ... and to notify the Department of Commerce." This element identifies whether the dispute resolution body or privacy program has a mandatory referral provision in its rules.

APPENDIX II

Analytical Criteria for Privacy Programs

A. *Incorporation of SH notice principles in privacy program rules*

The first group identifies whether the privacy program incorporates the SH notice principles in the program's rules of membership. The results of the analysis of this group are included in Table A of Appendix III. These elements are:

- Member's policy provide program contact information (Yes/No)
- Member's policy must state compliance with SH (Yes/No)
- Member's policy must be clear and conspicuous (Yes/No)
- Member's policy must specify the purposes for data processing (Yes/No)
- Member's policy must disclose 3rd party recipients (Yes/No)
- Members must provide data subjects with choice for use and dissemination of personal information (Yes/No)

B. *Incorporation of SH choice principles in privacy program rules*

The second group identifies whether the privacy program incorporates the SH choice principles in the program's rules of membership. The results of the analysis of this group are included in Table B of Appendix III. These elements are:

- Member's policy must provide opt-out for 3rd party disclosures (Yes/No)
- Member's policy must provide opt-out for secondary use (Yes/No)
- Members must offer clear and conspicuous choice (Yes/No)
- Members must provide the choice in a readily available manner[118] (Yes/No)
- Members must provide choice in an affordable manner (Yes/No)
- Member's policy must provide opt-in for sensitive data (Yes/No)

C. *Incorporation of SH onward transfer principle in privacy program rules*

The third group identifies whether the privacy program incorporates the SH onward transfer principle in the program's rules of membership. The results of the analysis of this group are included in Table C of Appendix III. These elements are:

[118] "Readily available" means that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out.)

- Members must provide notice of onward transfers (Yes/No)
- Members must provide choice for onward transfers (Yes/No)
- Members must obtain 3rd party processor's commitment to comply with the SH principles (Yes/No)

D. *Incorporation of SH security and integrity principles in privacy program rules*

The fourth group identifies whether the privacy program incorporates the SH security and integrity principles in the program's rules of membership. The results of the analysis of this group are included in Table D of Appendix III. These elements are:

- Members must take reasonable Security Precautions (Yes/No)
- Members restrict their processing to relevant data (Yes/No)
- Members only process data for purposes that are compatible with the specified purpose or that are authorized by the data subject (Yes/No)
- Members must take steps to ensure the reliability if data for the intended use (Yes/No)

E. *Incorporation of SH access principle in privacy program rules*

The fifth group identifies whether the privacy program incorporates the SH access principle in the program's rules of membership. The results of the analysis of this group are included in Table E of Appendix III. These elements are:

- Members must provide reasonable access to data subjects for their personal data (Yes/No)
- Members may a reasonable fee for access (Yes/No)
- Members must provide for correction of inaccurate data (Yes/No)
- Members must provide for the amendment of inaccurate data (Yes/No)
- Members must provide for the deletion of inaccurate data where appropriate (Yes/No)

F. *Incorporation of SH enforcement principles in dispute resolution including FAQ 11*

The fifth group identifies whether the privacy program and its dispute resolution body, if any, incorporate the SH enforcement principles, including those specifically enumerated in FAQ 11. The results of the analysis of this group are included in Table F of Appendix III. These elements are:

- The Privacy Program provides an Independent Dispute Resolution Body ("DRB") for individuals' complaints about members (Yes/No)
- The DRB must investigate of each complaint (Yes/No)

- Privacy Program offers readily available and affordable Recourse (Yes/No)
- Privacy program recourse procedures are transparent for data subjects (Yes/No)
- DRB can require the reversal of the effects of non-compliance with the Member's privacy policy (Yes/No)
- DRB can obtain a commitment that future processing be compliant with SH (Yes/No)
- DRB can require the cessation of non-conforming processing (Yes/No)
- DRB can order compensation for harm caused by non-compliant processing (Yes/No)
- Privacy Program can sanction Members (Yes/No)
- DRB publishes all decisions containing sanctions (Yes/No)
- DRB refers sanctioned cases to governmental authorities when member fails to take corrective action (Yes/No)

APPENDIX III

Questionnaires for in-depth study of company practices

1-Party responsible for the transfer in the country of origin (sender)

A. Type of business

2-Recipient of the data in the third country

A. commercial (specify)

B. HR (specify)

C. research (specify)

D. travel (specify)

E. other (specify)

3-Characteristics of the data transferred

What is the number of concerned persons on the file per transfer?

What is the number of items of information transferred?

What is the content of the data transferred?

*Identification data (name, address, telephone number, identity card, driver's license, etc.) provide details.

*Personal characteristics (age, sex, marital status, physical data, nationality, immigration status, military status, household composition, leisure and interests, consumption habits, education and training, etc.). Provide details.

*Data relative to profession and employment (current employment, details as to termination of employment, attendance and disciplinary history, salary, evaluation, etc.). Provide details.

*Medical data (relative to physical o psychological state of health, to the situations and behaviours at risk, to the medical background, etc.). Provide details.

*Data relative to the sexual behaviour of the person on file. Provide details.

*Data relative to the racial or ethnic origin of the person on file. Provide details.

*Data relative to the religious, philosophical or political convictions of the person on file. Provide details.

*Data relative to the union affiliation of the person on file. Provide details.

*Other data category. Provide details.

4-Purpose of the transfer

A.What is the purpose of the transfer?

*Company management (personnel administration, planning of activities, clientele management, management of litigations, public relations, technical-commercial information, etc.). Provide details.

*Commerce (mail order sales, customer profiling, direct marketing, etc.). provide details.

*Teaching and culture (student administration, library administration, etc.). provide details.

*Health care

*Scientific research (epidemiological research, bio-medical research, sociological research, etc.). provide details.

*Other aims (to be identified).

B.Is the purpose of the posting in the third country identical to that pursued by the transmitter of the data?

5-Periodicity of the flow

A.What is the frequency of the transfers for which the authorisation is requested?

*Permanent, (specify)

*Regular, (specify)

*Exceptional (specify)

6-Duration of storage

A.No storage (immediate destruction).

B.Limited storage (in this case, specify the storage duration in months and in years, the aim of the storage, for example, for the purpose of proof).

C.Unlimited storage duration (specify the reasons).

7-Means of transfer

What is the chose means of transfer (on-line network, physical, etc.)?

If it involves a network, does it involve a closed (e.g.: Galileo) or an open (Internet) network? Provide details.

8-Security

A. Please describe the security measures that your organization has implemented to provide adequate technical and organizational security.

9-Patriot Act and other laws

A.Please describe the concrete impact of the Patriot Act (or other national security regulations) as regards personal data you receive from the EU.
B.Has your company ever limited the adherence to the SH principles (a) to meet national security, public interest, or law enforcement requirements (b) due to any statute, government regulation, or case law that create conflicting obligations or explicit authorizations? If yes, provide details.

10-Notice

A. How does your organization implement the Notice principle?
B. At what moment does your organization provide notice?
C.How does your organization determine the purposes for which it collects and processes personal data?
D.What standard does your organization use to afford clear and conspicuous notice (e.g. have the notice read by non-lawyers before it is posted on the website)?

11-Choice

A.How does your organization implement the Choice principle?
B.How does your organization assess the (non-)compatibility of a subsequent purpose with the original one?
C.Does the opt-in requirement for sensitive data processing create practical problems?
D.Does opt-out permit an individual to exercise choice at any time?

12-Onward Transfers

A.In the case you transfer data to a third party, does this party subscribe to the principles, is subject to the directive, another adequacy finding or do you enter into a written agreement with that third party.
B.How do you conduct onward transfers to data controllers (under SHA)?
C.How do you conduct onward transfers to data processors (under SHA)?

13-Data Integrity

A.How do you apply the data integrity principle, given the fact that the SH principles do not contain the purpose specification principle?

14-Access and Rectification

A.How do you implement access and rectification? Could you please describe the procedures you offer to data subjects?
B.How many access requests have you received? Have you encountered problems in administering access and rectification?

15-Enforcement

A.What is/are the mechanism/s you have chosen for assuring compliance with the SH principles?
B.What recourse/s it/they provide for individuals affected by non-compliance?
C.Are these mechanisms readily available?
D.Are they affordable? How much would they cost to the data subject?
E.Are damages foreseen in the applicable law or private sector initiative?
F. What are the follow-up procedures for verifying that the attestations and assertions your company make about its privacy practises are true and have been implemented as presented?
G.What would be the consequences/sanctions for your organization in the case of non-compliance?

16-Sensitive data

A.In case you process sensitive data, do you give opt-in?

17-Journalistic exception

A.Have you ever apply the journalistic exception? If yes, under what circumstances?

18-Cooperation with European DPAs

A.Have you committed to cooperate with European DPAs? If yes, have any cooperation been concretely asked? If yes, what kind of cooperation? What was the outcome?

19-Certification

A.Do you provide self-certification letters on an "annual" basis?

20-Verification

A.Which verification procedure has your company chosen?
B.Do you provide for the "annual" verification?

21-Human Resources data

A.In case you transfer HR data, what is the purpose of such transfer?
B.Do you disclose it to third parties?
C.Do you use it for different purposes?
D.How do you implement "notice" and "choice" principles in those cases?
E.Do you anonymize certain data, assigned codes or pseudonyms when the actual names are not required for the management purpose at hand?
F.Have you ever deny an "access" requirement asked by an employee? If yes, under which basis?

22-Controller to processor

A.In case you transfer data to a processor located in the US under the SH principles, do you also signed a contract regulating this issue?

23-Travel data

A.Is travel data transferred?
B.If yes, have your company been asked access to these data by US public bodies?

24-Pharmaceutical and Medical data

A.In case you transfer pharmaceutical and/or medical data, is these data used for new scientific research activity?
B.Have individuals asked to withdraw from a clinical trial?
Which use do you make of these data?

25-Public record and publicly available information

A.Does your company transfer data from Public record or publicly available information?

26-Internal Communication and Management of the SH Principles

A.How do you concretely train your employees to ensure that your organization effectively respects the SH principles (internal guidelines, employee education, software architecture (e.g. pop=ups), employee notices, etc.)?

27-Reason for joining the SH

A.What has been the reason for your company to join the SH?

28-Procedure

A.Did you find the procedure for joining: difficult, bureaucratic, simple, etc.?

29-Problems

A.Have you experienced any problem after joining the SH? If yes, could you describe/explain the nature?

APPENDIX IV

Questionnaires to different parties involved in the SHA system

a) Questionnaire to Lawyers (confidentiality of their names guaranteed)

1) What do you consider to be the advantages of the SHA regime when you contemplate a corporate data transfer strategy?
2) What do you consider to be the disadvantages of the SHA regime when you contemplate a corporate data transfer strategy?
3) Do you consider that the European Commission Decisions on Model Contractual Clauses have any impact on the strategy concerning TBDF? Why?
4) Do you believe that the SHA sstem results in a double data protection regime within companies (one of EU data and one of US data), or do you rather experience that companies increase the US data protection regime to the SH regime or beyond it?
5) How do you implement the yearly certification and verification requirements (internally or via a third party auditor; please describe the internal procedure)?
6) Have you been confronted with enforcement actions (including investigative questions) of European DPAs in the context of data transfers under the SH regime? If yes, what was the outcome?
7) Have you been confronted with enforcement actions (including investigative questions) of the FTC (or any other US public body) in the context of the SH regime? If yes, what was the outcome?
8) What complaint and mediation procedure do you prefer (BBBonline, TRUSTE, DMA, or other? Why? Which elements do you consider when you chose between these providers?
9) Do you have experience with data protection complaints before such private bodies? If yes, what was the result? Do you believe they function well?
10) How do you generally provide access to data subjects (via data exporters or data importers?
11) Do you believe that the SH regime offer a feasible solution to conduct: =processor to processor transfers? =controller to processor transfers?
12) Have any of your clients experience limitations in the adherence to the SH principles due to (a) necessity to meet national security, public interest, or law enforcement requirements (b) due to any statute, government regulation, or case law that create conflicting obligations or explicit authorizations? If yes, provide details.

b) Questionnaire to European DPA

1) Is notification of data transfers required pursuant to the data protection act (or otherwise) of your country? If yes, please specify the legal basis and procedure of such notification. Does such notification require that your mention the legal basis (including the SHA) on which personal data is transferred to the third country?
2) If notification is required, please mention how many data transfers under he SHA regime have been declared to your institution.
3) Can you specify the data transfer categories that are notified to your institution, and the exact amount of notifications for each category (e.g. 25 HR data, 12 consumer data, etc.)?
4) Can you specify how many of the SH notifications concern intra-company transfers and how many concern third company transfers?
5) Do you treat SH transfers differently if he harbourite has announced not to cooperate with European DPAs? If yes, could you specify the differences?
6) Has your organization published any specific guidelines and/or opinions for companies that want to use the SH regime? If yes, could you provide a copy of them?
7) Has your organization received any complaint regarding the transfer of personal data under the SH regime? If yes, could you please specify how many complaints you have received and from whom you received the complaint (data subject, consumer protection organization, data exporter, other)? What was the nature/reason of the complaint? How are such complaints treated? Has your organization got procedures in place to investigate compliance with the SHA and to coordinate such investigations with the FTC? What has been the outcome of such a complaint procedure?
8) Has your organization received any communication from the FTC to investigate data streams under the SH regime (for instance, where a data subject's complaint is investigated by the FTC but needs input of your organization)?
9) Has your organization ever approached the FTC to monitor and/or investigate compliance with the SHA?
10) Has your organization ever suspended data flows under Article 3 of the SHA? If yes, why?
11) Is there any information procedure foreseen for he application of Article 3.1.a) of the SHA? If yes, could you describe it?
12) Are you assessing/have you assessed the extent to which the adherence to the SHA principles may be limited for purposes of national security, public interest, or law enforcement requirements, as mentioned in the introduction to the SH principles?
13) How many people within your institution work with international data transfers?

c) Questionnaire to the FTC

1) Have you received any complaint concerning the application of the SHA? If yes, from who (directly from the data subject, ADR/ODR bodies, competitor companies, data exporter, European DPA, consumer association, etc.)? can you describe the nature and outcome of the complaint/s?
2) Do you have procedures in place o deal with such complaints? If yes, can you please describe them?
3) Is there any fee for submitting a complaint? If yes, how much does it cost (approximately)?
4) Can you take preliminary actions during the procedure? If yes, please describe them.
5) What type of sanctions can the FTC impose?
6) Have you contemplated any type of communication procedure with European bodies (European Commission, European DPAs, Article 29 Working Party, etc.) for better implementation of enforcement procedures?
7) Is there any special group/task force within your organization dealing with privacy issues? If yes, can you please describe their function regarding the SHA?
8) Is there any law passed after the adoption of the SHA that could limit adherence to the principles due to (a) necessity to meet national security, public interest, or law enforcement requirements (b) due to any statute, government regulation, or case law that create conflicting obligations or explicit authorizations? If yes, provide details. What are the parameters for the application of the "necessity test" that would have to be conducted as described by the exception included in the introduction to the SH principles?

d) Questionnaire to Consumer Organization

1) Have you ever received a complaint connected to the use of personal data transferred under the SHA? If yes, could you please describe it? If no, what do you think is the reason for a lack of complaints?
2) In case you receive a complaint, what would/have you do/done?
3) Have you made any analysis/report/survey concerning the implementation of the SHA from a Consumer law point of view? If yes, could you provide a copy of them or a description of the main findings/outcome?
4) Do you think that when a consumer is targeted in their own language, and data concerning him is transferred under the SHA, would not be necessary to provide notice in the same language? If yes, what is the legal basis? Do you think this issue has an impact on complaints/enforcement of the SHA agreement? Why?

e) Questionnaire to the DoC

1) Do you make any kind of review of the information contained in the SH self-certification declarations?
2) If yes, could you please describe the review procedure (e.g are incomplete cerifications refused; do you control consistency between the information provided in the self-certification form-letter and the privacy policy of the company; etc)?
3) Have you received any notification of company's persistent failure to comply with the SH Agreement sent by any enforcement body (public or private) ?
4) What is the procedure you follow when a company does not respect the annual verification?
5) Have you withdraw any company from the list?
6) If yes, do you keep record of those companies? Is this notified to the FTC and or DPA Panel?
7) Is the record of withdrawn companies (if any) made publicly available, for instance, on the webiste?

f) Questionnaire to ADRs

1) Has your organization competence to investigate SHA consumer privacy complaints?
2) Could you please explain how consumers may deposit a SHA complaint with your organization?
3) Does your organization provide for forms and procedures in different languages?
4) What is the price for an arbitration/ADR procedure (for both companies and consumers) in SHA dispute?
5) What are the selection criteria for panel members/arbiitrators?
6) Have there been any SHA procedures so far? Do you have any available statistics?
7) May a dispute settlement procedure lead to an obligation of companies to reverse any effects of a violation of the safe harbor principles? What other sanctions can be imposed to companies?
8) Are decisions/sanctions on SHA dispute settlements made publicly available?

APPENDIX V

Data Tables and Graphics of Point 2 (Certification Page Analyses)

Compan	a) Ind sect	b) Data type	Contr oller/ Proc essor	c) Personal data	d) Accur	f) verif	g) Reg	h) Priv. Prog	i) DR	j) Co	k) certif
	CSV	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	ADV	C, pro	pro	on, off, MP	Y	in-h	FTC	DMAshp	DMAshp	no	Current
	TES	C	cont	off	NDL	in-h	FTC	N/A	DPA	no	Current
	MCS	C, RH, pro	pro	on, off, HR	No	in-h	both	no	DPA	Y	Current
	ADV	RE	cont	on, off	NDL	in-h	FTC	DMAguid	DMAshp	no	Current
	DRG, BTC, HCS	RE	cont	on, off, MP	NDL	in-h	FTC	HON, TRUSTe	DPA	no	Current
	CSV, INF	C, pro	pro	on, off, MP	NDL	in-h	FTC	no	DMAshp	no	Current
	CPT, CSF	HR	cont	on, HR	NDL	in-h	both	TRUSTe	DPA, TRUSTe	no	Current
	FNS	C	cont	off, MP	PA	in-h	FTC	no	DPA	Y	Current
	TEL, TES, CSF	HR	cont	HR	Intranet	in-h	error	N/A	DPA	Y	Current
	CSV, FNS	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	CSV, CSF	C, pro	pro	on, off	Y	in-h	FTC	no	DPA	Y	Not
	DFN, INF, TES	C	cont	on	Y	TP	FTC	TRUSTe	TRUSTe	no	Current
	EIP, ELC, BTC	HR, C	cont	on, off, HR, MP	Y	in-h	both	BBB	BBB, DPA	no	Current
	TRA	T, pro	pro	on	NDL	TP	FTC	no	DPA	Y	Current
	INF	C, HR	cont	on, off, HR	Intranet	in-h	both	no	DPA	Y	Current
	GSV	RE	cont	on, off, MP	Y	in-h	FTC	CASRO	DPA	Y	Current
	HCS, INF	RE	cont	on, off	Y	in-h	FTC	no	BBB	no	Current
	INS, EDS, GST	?	cont	on, off, MP	PA	in-h	FTC	no	DPA	Y	Current
	ADV, TRN, INF	C	cont	on	Y	in-h	FTC	AAA	AAA	no	Current
	CSV, INF, HCS	RE, M	cont	on	NDL	TP	FTC	BBB	BBB	no	Current
	GCG, INF	C	cont	on, off, MP	NDL	in-h	FTC	no	BBB	no	Current
	EDS, TRA	C RH, M	cont	on, off, HR, MP	Y	in-h	both	BBB, TRUSTe	BBB, TRUSTe, DPA	no	Current
	ACR, APS, PVC	C, HR	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	BTC	R, HR, C	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	MED, DRG	R, HR, C	cont	on, off, HR, MP	No	in-h	both	no	DPA	Y	Current
	CSF	HR	cont	on	Y	in-h	both	no	DPA	Y	Current
	CSF, CSV, INF	C	cont	on, off, MP	Y	TP	FTC	TRUSTe	TRUSTe	no	Not
	CSV	C, pro	pro	on, off	No	in-h	FTC	no	DPA	Y	Current
	BOK, ADV	C, pro	pro	on	No	in-h	FTC	DMAshp	DMAshp	no	Current
	APS	HR	cont	HR	Y	in-h	error	no	DPA	Y	Current

	CSF, CSV, CPT	C RH	cont	on, HR	Y	in-h	both	no	DPA for HR	Y	Current
	ADV, CSF	C	cont	,	Y	TP	FTC	NAI, TRUSTe	TRUSTe	no	Current
	CSF	C RH	cont	on, off, HR	NDL	in-h	both	no	BBB, DPA	Y	Current
	ADV	C	cont	on, off	NDL	in-h	FTC	TRUSTe	TRUSTe	Y	Current
	GCG	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	TRA, GSV, MCS	C RH	cont	on, off, HR	Y	in-h	both	no	DPA	Y	Current
	EDS, CSV, CSF	C RH	cont	on, off, MP	NDL	TP	FTC	TRUSTe	TRUSTe	Y	Current
	MED, DRG, BTC	C, HR	cont	on, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	CSF	HR	cont	HR	Intranet	in-h	error	N/A	DPA	Y	Current
	ACE	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	CSV, INF, CSF	HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	ADV, INF	C	cont	on, MP	AUR	in-h	FTC	no	DPA	Y	Not
	INF, CSV	C	cont	on, off, MP	Y	in-h	FTC	BBBOnL	DMAshp	no	Current
	TRA	T	cont	on, off	NDL	in-h	FTC	BBBOnL	BBB	no	Current
	ADV, INF, GSV	C, pro	pro	on off	Y	in-h	FTC	CAUCE, AIM	TRUSTe	no	Current
	HCS MED	HR, C	cont	on, off, HR, MP	No	in-h	both	N/A	DPA	Y	Current
	INF,CFS	C	cont	on, off	NDL	in-h, T	FTC	NAI	BBB, DPA	Y	Current
	INF, CSV, TES	C	cont	on, off	NDL	in-h	FTC	no	DPA	Y	Current
	EDS	C	cont	on, off	Y	in-h	FTC	BNI	DPA	Y	Current
	APS	HR	cont	,	,	in-h	error	no	DPA	Y	Current
	ADV	C	cont	on	Y	in-h	FTC	TRUSTe	TRUSTe	no	Current
	INV, ADV, EDS	HR, C	cont	on, HR	Y	in-h	both	GBCC	BBB	Y	Current
	HCS	C	cont	on	NDL	TP	FTC	TRUSTe	TRUSTe	no	Current
	CFS, CVS	C	cont	on	NDL	TP	FTC	TRUSTe, BBB	TRUSTe	no	Current
	ADV	C	cont	on, off	Y	in-h	FTC	no	DMAshp	no	Not
	EDS, CSV, MCS	HR	cont	HR	AUR	in-h	error	no	DPA	Y	Current
	CSF, CSV, GSV	HR	cont	on, HR, MP	PA	in-h	both	no	DPA	Y	Not
	CSV	C, pro	pro	on	PA	in-h	FTC	no	DPA	Y	Current
	CSF, MED	C RH, M	cont	on, HR	NDL	in-h	both	BBB	BBB, DPA	Y	Current
	ACE, TES, OMS	HR	cont	HR	Intranet	in-h	error	DoC	DPA	Y	Current
	CSF, CSV	C	cont	on, off, MP	NDL	TP	FTC	DMAshp, TRUSTe	DMA, TRUSTe	Y	Current
	INF	C	cont	on	Y	TP	FTC	TRUSTe, HON	TRUSTe, HON	no	Current
	CSV	C, pro	pro	on	Y	TP	FTC	TRUSTe	TRUSTe	no	Current
	CSV, GSV, INF	HR, C	cont	on, off, MP	PA	in-h	FTC	no	DMAshp	Y	Current
	CSF, CSV, INF	C	cont	on	Y	in-h	FTC	no	DPA	no	Current
	INF	HR	cont	HR	Y	in-h	error	N/A	DPA	Y	Current

	AGM, CON, FNS	HR	cont	HR	Y	in-h	error	no	DPA	Y	Current
	GIE, EIP, TEL	HR	cont	on, off, MP, HR	NDL	in-h	both	no	DPA	Y	Current
	CSV, CSF	R, pro	pro	off, MP	AUR	in-h	FTC	no	BBB	no	Current
	ARW, CSF, INS	C	cont	on, off, MP	Y	in-h	FTC	no	DPA	Y	Current
	CSF, CSV	HR, pro	pro	on, HR	No	in-h	both	no	DPA	Y	Current
	CSV, MCS, INF	HR, RE	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	CPT, CSC	C	cont	on	NDL	in-h	FTC	no	AAA	no	Current
	CSV	HR	cont	on, off, HR, MP	Intranet	in-h	both	no	DPA	Y	Current
	TES	C	cont	on	Y	in-h	FTC	no	AAA	no	Current
	INF	C, RH	cont	on, off, HR, MP	AUR	in-h	both	no	DPA	Y	Current
	GSV, GCG	C, pro	pro	off, MP	Y	in-h	FTC	no	DPA	Y	Current
	AVS	T	cont	on	Y	TP	DoT	BBB	BBB	no	Current
	OGS, OGM, CSF	HR, C	cont	on, off, HR, MP	NDL	in-H	both	no	DPA	Y	Current
	CSV, INF, CSF	C	cont	on	Y	in-h	FTC	TRUSTe	TRUSTe	no	Current
	CSV, INF	C, RH, pro	pro	on, off, HR	Y	in-h	both	no	DPA	Y	Current
	CSV, TRA	T, pro	pro	on	No	TP	FTC	N/A	TRUSTe	no	Current
	GSV, MCS, TRA	R RH	cont	on, off, HR	No	in-h	both	no	DPA	Y	Current
	CSV	C, pro	pro	on, off	NDL	in-h	FTC	DMA	DMAshp	no	Current
	APP, HCG, ARW	C RH	cont	on, off, HR	Y	in-h	both	no	DPA	Y	Current
	INF	C	cont	on, off	NDL	in-h	FTC	TRUSTe	TRUSTe	no	Not
	TRN, PRT, RRE	C, HR, RE	cont	HR	NDL	in-h	error	no	DPA	Y	Current
	APS, GIE, TRK	HR	cont	HR	No	in-h	error	no	DPA	Y	Current
	CSV, CSF, INF	C	cont	on	NDL	in-h	FTC	TRUSTe	TRUSTe	no	Current
	CSV, CSF	C, pro	pro	on	Y	in-h	FTC	?	DPA	Y	Not
	INF, GSV, HCS	? RH	cont	on, off, HR	No	TP	both	no	USERTRUST	Y	Current
	EDS, CSF, CSV	HR	cont	on, HR	NDL	TP	both	TRUSTe	TRUST, DPA	Y	Current
	MCS, ADV, GSV	RE	cont	on, off	Y	in-h	FTC	no	AAA	no	Current
	COL, ELP, FNS	HR	cont	HR	Intranet	in-h	error	N/A	DPA	Y	Current
	CSV	C, pro	pro	on, off	NDL	TP	FTC	DMAshp	DMA	no	Current
	DRG	?	cont	on	PA	in-h	FTC	BBB	BBB	no	Current
	CSV	C, pro	pro	on, off	NDL	TP	FTC	no	DMA	no	Current
	EDS, INF, BOK	C RH	cont	on, off, HR, MP	Y	in-h	both	DMA	DPA	Y	Current
	BOK, EDS, CSF	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	INF	RE	cont	on	Y	in-h	FTC	CASRO, MRA, ESOMAR, TRUSTe	TRUSTe, DPA	Y	Current
	CSF, CSV	HR	cont	HR	PA	in-h	error	no	DPA	Y	Current
	MCS, ACE	HR	cont	on, off, HR, MP	Intranet	in-h	both	no	DPA	Y	Current

	ADV, GSV	HR, C	cont	on, off, HR	Y	in-h	both	TRUSTe, DAMshp, AIM, Cre-m, NAI	DMA, TRUSTe	Y	Current
	CSF, CSV	RH	cont	off	P	in-h	FTC	no	DPA	Y	Current
	CSF, ADV, INF	C	cont	on, off	Y	in-h	FTC	DMA	DMA	N/A	Current
	ADV	C	cont	on, off	Y	in-h	FTC	DMA	DMA	no	Current
	CVS	HR	cont	on off, HR	PA	in-h	both	no	DPA	Y	Current
	ADV, TRN	C	cont	off	Y	in-h	FTC	no	DPA	Y	Current
	FNS,GSV,ACT	C	cont	on	NDL	TP	FTC	no	DPA	Y	Current
	ADV, CSF, INF	C	cont	on, off	NDL	in-h	FTC	DMA	DMA	no	Current
	ADV	C	cont	on, off, MP	NDL	in-h	FTC	DMAshp	DMAshp	N/A	Current
	INF	RE	cont	on	NDL	TP	FTC	TRUSTe	TRUSTe	no	Current
	GSV	HR, C	cont	on, off	Y	TP	FTC	TRUSTe	TRUSTe	Y	Current
	EMP	RE	cont	on, off, MP	Y	in-h	FTC	no	BBB	no	Current
	PHT, CPT	C, HR, RE	cont	on, off, HR, MP	Y	in-h	both	BBB	BBB, DPA	Y	Current
	APS, ELC, GIR	HR	cont	HR	PA	in-h	error	no	DPA	Y	Current
	TES	HR	cont	HR	Intranet	in-h	error	N/A	DPA	Y	Current
	MED, DRG	HR	cont	HR	PA	in-h	error	no	DPA	Y	Current
	CSV	C	cont	on, HR	Y	TP	both	no	AAA	Y	Current
	CSF, TOY	C, RE	cont	on, HR	Y	TP	both	ESRBPOP	ESRBPOP	Y	Current
	GST, ICH, BTC	C	cont	on	No	in-h	FTC	BBB	BBB	Y	Current
	EDS, FNS	HR	cont	on, HR	Y	TP	both	TRUSTe	TRUST, DPA	Y	Current
	LES, TRN, AUT	C	cont	on	NDL	in-h	FTC	BBB	BBBOnL	Y	Current
	CSF, INF, EDS	C	cont	on	Y	in-h	FTC	no	Eftpeb	no	Current
	CSF	C	cont	on	NDL	in-h	FTC	no	DPA	Y	Current
	ACT, EDS, GSV	C, HR	cont	on, off, HR, MP	Y	in-h	both	BBB	BBB	Y	Current
	CSF	C	cont	on	No	in-h	FTC	no	DPA	Y	Current
	CPT, CSF, CSV	HR	cont	off, HR, MP	Intranet	in-h	both	no	DPA	Y	Current
	CSF	HR	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	CSF, CSV, CST	C, RE	cont	on, off	Y	TP	FTC	TRUSTe	TRUSTe	no	Current
	GSV, INF, MCS	HR	cont	on, off, HR, MP	NDL	in-h	both	N/A	DPA	Y	Current
	EIP, GST, LAB	HR	cont	HR	Y	in-h	error	no	DPA	Y	Current
	CSF, GSV	HR	cont	on, off, HR	Y	in-h	both	N/A	DPA	Y	Current
	CSV, INF	C	cont	on, off	Y	in-h	FTC	no	AAA	no	Current
	CSV, CSF, INF	HR	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	PVC	HR	cont	on, off, HR, MP	Intranet	in-h	both	no	DPA	Y	Current
	CSF	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	FOT, APP, SPT	HR	cont	HR	No	in-h	FTC	no	DPA	Y	Current

	EDS, CSF	C	cont	on, off, MP	NDL	in-h	FTC	no	DPA	Y	Current
	CSF, INF, MCS	RE (HR & C	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	MCS, GSV	HR	cont	on, off	Y	in-h	both	AAA	AAA	Y	Current
	CPT, CSV	HR, C	cont	on, HR, MP	Y	in-h	both	no	DPA	Y	Current
	CSV, TRA, INF	C, T, RH	cont	on, off, HR	Y	TP	both	TRUSTe	TRUSTe	Y	Current
	GSV, TOY	C	cont	on, off	No	in-h	FTC	no	DPA	Y	Current
	AUT, FNS, INS	C	cont	on, off	No	in-h	FTC	no	DPA	Y	Current
	GSV, CSV	RE RH	cont	on, HR, MP	No	in-h	both	no	DPA	Y	Current
	BTC, GST	RE, M	cont	on, MP	No	in-h	FTC	AABB	DPA	no	Current
	CSV, INF	pro	cont	on, off, MP	Y	in-h	FTC	DMA	DMA	no	Current
	MCS, CSV	pro	cont	on, off	Y	in-h	FTC	DMAshp	DMAshp	no	Current
	EMP	HR	cont	on, off, MP	AUR	in-h	both	no	DPA	Y	Current
	INF	RE	cont	on, off, MP	Y	in-h	FTC	no	JAMS	no	Current
	INF	H RH	cont	on, off, MP	Y	in-h	both	no	DPA	Y	Current
	HCS, MCS	C, M	cont	on, off, MP	Y	in-h	FTC	no	DPA	no	Current
	EDS, CPS	C, HR	cont	on, off, HR	Y	in-h	both	no	DPA	Y	Current
	CSF	C	cont	on, off, MP	NDL	in-h	FTC	no	DPA	Y	Current
	AIR	HR	cont	HR	PA	in-h	error	no	BBB	Y	Current
	GSV	RE	cont	on, off, MP	Y	in-h	FTC	TRUSTe	TRUSTe	Y	Current
	INF, CSF, CSV	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	INF, CSV, TOY	C RH	cont	on, HR, MP	NDL	in-h	error	no	DPA	Y	Current
	INF, CSV	C	cont	on, off, MP	Y	in-h	FTC	no	AAA	no	Current
	HCG, GFT, GCG	C	cont	on, off	Y	in-h	FTC	DMA	DMA	no	Current
	GSV	RE	cont	on, off, MP	NDL	in-h TI	FTC	TRUSTe	TRUSTe	Y	Current
	ADV, CSV, CSF	C	cont	on, off, MP	NDL	in-h	FTC	DMAshp	DMAshp	Y	Current
	ICH	HR	cont	HR	Intranet	in-h	error	N/A	DPA	Y	Current
	APP, TXF	C	cont	on, off, MP	NDL	in-h	FTC	DMA	DPA	Y	Current
	HCS	C, M	cont	on, off	Y	in-h TI	FTC	HON	DPA	no	Current
	CPT, CEL, CSF	C, HR	cont	on, off, HR, MP	Y	in-h	both	BBB	BBB, DPA	Y	Current
	CSV, TRA, INF	T, RH	cont	HR	PA	in-h	error	no	DPA	Y	Current
	EMP	HR	cont	HR	Y	in-h	error	TRUSTe	DPA	Y	Current
	CSV, EMP	HR	cont	HR	No	in-h	error	SSN	DPA	Y	Current
	CSF, CSV	HR	cont	on, off, HR	NDL	in-h	both	no	DPA	Y	Current
	CSF, INF	HR	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	INF, CSV	HR	cont	HR	Intranet,	in-h	error	EPON, EPOF, IAPO, SHRM, CLSR	DPA	Y	Current
	DRG, BTC	HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current

	AUV, CPT, CEL	C, HR	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	INF	C	cont	on, HR	NDL	in-h	both	no	no	Y	Current
	EDS, INF, EMP	HR	cont	on, HR	NDL	in-h TI	both	TRUSTe	TRUSTe	Y	Current
	GSV	RE	cont	on	Y	in-h	FTC	TRUSTe	TRUSTe	no	Current
	ACE	HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	INF	C, T, RH	cont	off, HR, MP	No	in-h	both	no	CFO, DPA	Y	Current
	EDS, CSV	HR	cont	on, HR	Y	in-h	both	no	DPA	Y	Not
	CPT, CSF, CEL	C, HR	cont	on, off, HR, MP	Y	in-h	both	BBB	BBB, DPA	Y	Current
	INF, GST, BTC	C	cont	off, MP	NDL	in-h	FTC	no	DPA	Y	Current
	MCS, INF	HR	cont	on, off, HR, MP	AUR	in-h	both	no	DPA	Y	Current
	ACE, ELP, REQ	HR	cont	HR, MP	Intranet	in-h	both	no	DPA	Y	Not
	CSF, CSV, ACE	C, RH	cont	on, off, HR, MP	Y	in-h	both	NAITA	TRUST, DPA	Y	Current
	CSV, CPT, CSF	C, RE	cont	on	NDL	in-h	FTC	TRUSTe	TRUSTe	no	Current
	INF, CSV, CSF	C, RH	cont	on	No	in-h	both	no	DPA	Y	Current
	CSV, INF	C, RE	cont	on	No	in-h	FTC	TRUSTe	TRUSTe	no	Current
	INF, MCS	C, HR, RE	cont	on, off	Y	in-h	both	N/A	AAA	Y	Current
	EDS	RE	cont	off	NDL	in-h	FTC	N/A	DPA	Y	Current
	CSV, ADV	C	pro	on, off, MP	No	in-h	FTC	DMAshp	DMAshp	no	Not
	APS, ELP, PCI	C, HR	cont	on, off, HR, MP	No	in-h	both	no	DPA	Y	Current
	INF	C	cont	on	Y	in-h	FTC	no	BBB	no	Current
	CVS, INF	C, RE	cont	both	NDL	in-h	both	no	AAA	no	Current
	EMP	C, HR	cont	on, off, HR	NDL	in-h	both	no	DPA	Y	Current
	CSV, INF, EMP	C, HR, RE	cont	on, off, HR	NDL	in-h	both	no	DPA	Y	Current
	ACT, CSV, INF	HR	cont	on, off, HR, MP	No	in-h	both	no	DPA	Y	Current
	GSV	C	cont	off	No	in-h	FTC	N/A	DPA	Y	Not
	GSV	,	cont	on, off	No	in-h	FTC	no	CASRO	no	Current
	EMP, INF	C, RE	cont	on, off, HR, MP	No	in-h	both	no	TRUSTe, DPA	Y	Not
	EMP	C, RE	cont	on, off	Y	in-h	FTC	no	BBB	no	Current
	CSV, INF	C	cont	on, off	NDL	in-h	FTC	no	DMA	no	Current
	TES, CSV, CSF	C, HR	cont	on, off, HR, MP	Y	in-h	both	PAB, TPC	DPA	Y	Current
	CSF, CSV	C, HR	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	CPT, CEL	C, RH	cont	on, HR	Y	in-h	both	TRUSTe	TRUSTe, DPA	Y	Current
	MCS, EDS	HR	cont	on, off, HR, MP	Y	TP	both	no	BBB, DPA	Y	Current
	INF, EDS, CSV	C	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	CSF	C, RH	cont	on, off, HR, MP	Y	TP	both	TRUSTe	TRUSTe, DPA	Y	Current
	MCS, EDS	C, RE	cont	on off	No	in-h	FTC	no	DPA	Y	Current

	GSV	RE	cont	on, off, MP	Y	in-h	FTC	CASRO	DPA	Y	Current
	INF, ADV, TEL	RE	cont	on, off	Y	in-h	FTC	CASRO, MRA	DPA	Y	Current
	TRA	C	cont	on, off	Y	in-h	FTC	no	DMA	no	Current
	TRA	C	cont	on, off	Y	in-h	FTC	no	DMA	no	Current
	CSV	C	cont	on	No	in-h	FTC	no	DPA	Y	Current
	CSV, TES	C	cont	on, off, MP	AUR	in-h	FTC	no	DPA	Y	Current
	DRG, CSF	C, HR	cont	on, HR	NDL	TP	both	PAB, IOPO, EPON	DPA	Y	Current
	HCS	C	cont	on	NDL	in-h	FTC	no	DPA	Y	Current
	GSV	RE, RH	cont	on, off, MP	Y	in-h	both	CASRO	DPA	Y	Not
	DRG	RE	cont	on, off, MP	NDL	in-h	FTC	no	DPA	Y	Current
	DRG, BTC	C, HR, RE	cont	on, off, HR, MP	Y	in-h	both	No	DPA	Y	Current
	CSF	C, RH	cont	on, off, MP	NDL	in-h	both	no	DPA	Y	Current
	ADV, HCS, INF	C, RE	cont	on, off, MP	NDL	in-h	FTC	DMAgui, HIPPA, COPPA	DMA	no	Current
	CSF, INF	C, HR	cont	on, off, HR, MP	Y	in-h TI	both	TRUSTe	TRUSTe, DPA	Y	Current
	EMP, CSV, CSF	HR, RE	cont	on, off, HR, MP	No	in-h	both	no	DPA	Y	Current
	GSV	RE	cont	on, off	NDL	in-h	FTC	CASRO, ESOMAR, MRA	DPA	Y	Current
	FNS	C, RH	cont	on, MP	NDL	in-h	both	no	AAA	Y	Current
	DRG, BTC, MED	C, RH	cont	on, HR, MP	No	TP	both	TRUSTe	TRUSTe	Y	Current
	BTC, GST, PCI	C, RE, RH	cont	off, MP	Y	in-h	both	no	DPA	Y	Current
	AIR, ELC	HR	cont	HR	PA	in-h	error	no	DPA	Y	Current
	CSV	C, RH	cont	on	NDL	in-h	both	no	DPA	Y	Not
	MCS	RE	cont	on, off, MP	Y	in-h	FTC	CASRO	DPA	Y	Current
	TRA	HR, T	cont	on, off, MP	Y	in-h	both	no	DPA	Y	Current
	CSV	C	cont	on, off, MP	Y	in-h	FTC	no	DPA	Y	Current
	CSV	C, pro	pro	on	Y	in-h	FTC	no	DPA	Y	Current
	EDF, CSV	C, HR	cont	on, off, HR	NDL	TP	both	TRUSTe	TRUSTe, DPA	Y	Current
	ADV, CSV, CSF	RE, RH	cont	on, off, HR	NDL	in-h	both	DMAshp	DMAshp, DPA	Y	Current
	INF, MCS, CSV	RE	cont	on	NDL	in-h	FTC	no	DPA	no	Current
	TES	C, RH	cont	on	No	in-h	both	no	DPA	Y	Current
	GSV	RE	cont	on, off, MP	No	in-h	FTC	CASRO	DPA	Y	Current
	GSV	RE	cont	on, off, MP	Y	in-h	FTC	CASRO	DPA	Y	Current
	GSV	RE	cont	on, off, MP	No	in-h	FTC	CASRO	DPA	Y	Current
	DFN, AIR, ELC	C, HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	CSF, CSV, EDS	C, RH	cont	on, off, MP	NDL	in-h	both	no	BBB, DPA	Y	Current
	ELC, CSF	HR	cont	on, HR	Intranet	in-h	both	no	DPA	Y	Current
	GCG, GSV	C, HR	cont	on, HR	Y	in-h	both	BBB	BBB, DPA	Y	Current

	DRG	C, HR	cont	on, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	INF	C, HR	cont	HR	Y	in-h	both	no	DPA	Y	Current
	ADV	C, RH	cont	on, MP	Y	in-h	both	no	DPA	Y	Current
	CSF	C	cont	on	PA	in-h	FTC	HIPPA	DPA	Y	Current
	CSF, INF	C, HR	cont	on, HR	Y	TP	both	TRUSTe	TRUSTe, DPA	Y	Current
	INF, HCS	C	cont	on, off	NDL	in-h	FTC	no	DPA	Y	Current
	DRG	RE, HR	cont	HR	Intranet	in-h	both	no	DPA	Y	Current
	MCS	C, HR	cont	HR	No	in-h	both	no	DPA	Y	Current
	GSV, MCS, TRA	C, RH	cont	on, off, HR	No	in-h	both	no	DPA	Y	Current
	CSF, CSV	C, HR	cont	on, HR	NDL	in-h	both	no	DPA	Y	Current
	CSV	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	GCG	C, RH	cont	on, off, HR, MP	NDL	in-h	both	DMA, DPA for HR	DMA, DPA	Y	Not
	GCG	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	CSV	C, HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	DRG	HR, RE	cont	on, off, MP	Y	in-h	both	no	DPA	Y	Current
	DRG	HR	cont	HR	NDL	in-h	error	IAPO	DPA	Y	Current
	DRG	C, HR	cont	on, off, HR, MP	NDL	In-h	both	no	DPA	Y	Current
	TES	C	cont	on	NDL	TP	FTC	TRUSTe	TRUSTe	no	Current
	CSF, CSV	C	cont	on, off, MP	NDL	in-h	FTC	no	BBB	no	Current
	ICH	C, HR	cont	on, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	CSV, CSF, TES	C, HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	ADV, CSV, CSF	C	cont	on, off	NDL	in-h	FTC	BBB, NAI, OPA	BBB, NAI, OPA	Y	Current
	APS, BLD, ICH	HR	cont	HR	PA	in-h	error	no	DPA	Y	Current
	GCG, HCG, CRM	C	cont	on, off, HR, MP	Y	in-h	both	no	DPA	no	Not
	DFN, ACE, GSV	RE, HR	cont	HR	NDL	in-h TI	both	ASISP, PIMC	DPA	Y	Current
	TRN, INF, MCS	T, RH	cont	off, HR	NDL	in-h	both	no	DPA	Y	Current
	BOK	C, HR	cont	on, off, HR, MP	NDL	in-h	both	no	AAA	Y	Current
	EMP	HR	cont	on, off, HR	Y	in-h	both	no	DPA	Y	Current
	GSV	HR	cont	on, HR	NDL	in-h	both	no	DPA	Y	Not
	COS, DRG, HCG	C, HR, RE	cont	on off, HR	Y	in-h	both	DMA, BBB	DMA	Y	Current
	CVS	C, HR, pro	pro	on, off	Y	in-h	both	no	BBB	no	Current
	INF	HR	cont	on, off, HR	No	in-h	both	no	DPA	Y	Current
	BOK, GCG	C	cont	off, MP	NDL	in-h	FTC	DMAshp	DMAshp	no	Current
	CSF, CSV, CPT	HR pro	pro	on, HR	Y	in-h	both	no	DPA	Y	Current
	DFN, AIR, ELC	HR	cont	HR	No	in-h	both	N/A	DPA	Y	Current
	CSF, CSV, INF	C	cont	on	Y	in-h	FTC	DMA	DMAshp	no	Current

	CSV, CSF	C, RE	cont	on	NDL	in-h	FTC	no	DPA	Y	Current
	CSV, TES	C	cont	on	NDL	in-h	FTC	no	AAA	no	Current
	INF, FNS, CSV	C, pro	pro	on off, MP	NDL	in-h	FTC	no	DPA	no	Current
	MED, HCS, CSF	C, RE, RH	cont	on, off	Y	in-h	both	P3P, CNIL member, HON	DPA	Y	Current
	PMR, GST	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	EMP, GSV	C, HR	cont	on, off, HR	NDL	TP	both	TRUSTe	TRUSTe, DPA	Y	Current
	CSV,	C, HR, RE	cont	on, HR	Y	TP	both	no	DPA	Y	Current
	CSV, INF	C, RH	cont	on, HR	NDL	in-h	both	TRUSTe	TRUSTe	Y	Current
	FNS, INF, CSV	RE, pro	pro	on	NDL	in-h	FTC	no	DPA	Y	Current
	CSV	? Pro	pro	on, off	Y	TP	FTC	TRUSTe	TRUSTe	no	Current
	CSV, ACT, INF	C, HR	cont	on, HR, MP	No	in-h	both	no	DPA	Y	Current
	GCG	HR	cont	on, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	GSV	C, RE	cont	on, off, MP	Y	in-h	FTC	CASRO	DPA	Y	Current
	ACE, AUT, MTL	HR	cont	on, off, HR	NDL	in-h	both	no	DPA	Y	Current
	CSV	C, RH	cont	on, HR	NDL	TP	both	TRUSTe	TRUSTe, DPA	Y	Current
	TEL, CPT, GIE	HR	cont	HR	Y	in-h	error	no	DPA	Y	Current
	CSF, CSV	RE, pro	pro	on	Y	in-h	FTC	TRUSTe	TRUSTe	no	Current
	CSV, INF	? Pro	pro	on, MP	Y	in-h	FTC	DMA Privacy Promise	DMA Privacy Promise	Y	Current
	HCS	RE	cont	on, off	No	in-h	FTC	no	DPA	Y	Current
	BOK	C	cont	on, off, MP	NDL	in-h	FTC	DMA	DMAshp	no	Current
	CPT, ELC, CSF	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	BOK	C	cont	on	NDL	in-h	FTC	no	DPA	no	Not
	AIR, ELP, ICH	HR	cont	on, HR, MP	PA	in-h	both	no	DPA	Y	Current
	CSV, CSF, INF	RE	cont	on, off, MP	No	in-h TI	FTC	TRUSTe	TRUSTe	Y	Current
	MCS	HR	cont	on, HR, MP	Y	in-h	both	no	DPA	Y	Current
	HCS, CSF, INF	RE, pro	pro	on, off	No	in-h	FTC	no	DPA	Y	Current
	CSF, CSV, INF	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	CSV, CSF, INF	C	cont	on, off, MP	Y	TP	FTC	TRUSTe, CAUCE, DMACfRe-mail	TRUSTe	Y	Current
	TRA	C, T	cont	on, off, MP	Y	in-h	FTC	no	DPA	Y	Current
	GSV	RE, HR	cont	HR	NDL	in-h	both	no	DPA	Y	Current
	GSV, GSF, INF	C	cont	on, off, MP	Y	in-h TI	FTC	TRUSTe	TRUSTe	no	Current
	GSV, CSV	C, pro	pro	on, off, MP	NDL	in-h	FTC	no	DPA	Y	Current
	APS, AIR	HR, pro	pro	HR	No	in-h	error	no	DPA	Y	Current
	CSF	C	cont	on, MP	NDL	in-h	FTC	DMA	DPA	Y	Current
	MED, HCS, CSF	HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	HCS	C	cont	on	No	in-h	FTC	no	AAA	no	Current

	BUS, CEL	C	cont	on, off, HR, MP	NDL	in-h	both	no	JAMS, DPA	Y	Current
	CPT, ELC, CSV	C, HR	cont	on, off, HR, MP	Intranet	in-h	both	no	DPA	Y	Current
	ARW, BOK, FLM	C	cont	on	Y	in-h	FTC	no	DPA	Y	Current
	GSV	RE	cont	on off, MP	Y	in-h	FTC	CASRO	DPA	Y	Current
	INF, CSV, CSF	C, pro	pro	on, off, HR	Y	in-h	both	no	DPA	Y	Current
	ADV, INF	RE	cont	on	NDL	in-h	FTC	UKTPS	AAA	no	Current
	CSF, CSV, EDS	C, HR	cont	on, off, HR	Y	TP	both	TRUSTe	DPA	Y	Current
	CSF	C	cont	on, MP	Y	in-h	FTC	no	DPA	Y	Not
	INF, CSV, EIP	C	cont	on	No	in-h TI	FTC	no	DPA	Y	Not
	GSV	HR	cont	HR	PA	in-h	error	no	DPA	Y	Current
	ADV	C, HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	AIR, FNS, GIE	HR	cont	HR	Y	in-h	error	no	DPA	Y	Current
	EMP	HR	cont	on	Y	in-h	FTC	no	DPA	Y	Not
	INS	C	cont	on, off	contract	in-h	FTC	no	TRUSTe	no	Current
	CSV	pro	pro	MP	NDL	in-h	FTC	no	DMA	no	Current
	ADV	C	cont	on	No	in-h	FTC	no	DPA	Y	Current
	INF	C	cont	on, off, MP	No	in-h	FTC	BBB	BBB	no	Current
	BTC, INF	RE	cont	on, off, MP	NDL	in-h	FTC	CFR, BR, DHHR	DPA	Y	Current
	EDS, HCS	RE	cont	on	NDL	in-h	FTC	no	DPA	Y	Current
	GSV, ACT	C	cont	on	Y	TP	FTC	TRUSTe	TRUSTe	no	Current
	CGC, FOD	C	cont	on, off, MP	NDL	in-h	FTC	no	AAA	no	Current
	INF	RE	cont	on, MP	Y	in-h	FTC	no	DPA	Y	Current
	INF, GSV, HCS	? pro	pro	on, off, HR	No	in-h	both	no	USERTRUST, DPA	Y	Current
	INF	C	cont	on	Y	in-h	FTC	TRUSTe	TRUSTe	no	Current
	LAB, INF, GST	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	CSF	C	cont	on, off, HR, MP	Y	in-h	both	no	DPA	Y	Current
	BOK	C, pro	pro	on, off	,	in-h	FTC	DMAshp	DMAshp	no	Not
	CSV, INF	C	cont	on	NDL	in-h	FTC	TRUSTe	TRUSTe	no	Current
	INF, MCS	C	cont	on	Y	in-h	FTC	KPMG, CIDE, CSPSTI	AAA	no	Current
	TRA, INS	T	cont	on, off, MP	Y	in-h	FTC	no	DPA	Y	Current
	INF	C	cont	on, off	Y	in-h	FTC	BBB	BBBOnL	no	Current
	CSV, INF	C	cont	on off	Y	in-h	FTC	no	Eftpeb	no	Current
	APS	HR	cont	on, off, HR	Intranet	in-h	both	no	DPA	Y	Current
	CSV, TRA	C	cont	on, off, HR	PA	in-h	both	no	DPA	Y	Current
	TRA	C, T pro	pro	on	NDL	in-h	FTC	no	DPA	Y	Current
	CSV, TRA	C, T	cont	on, off, HR, MP	AUR	in-h	both	no	DPA	Y	Current

	HCG, COS, FOD	HR	cont	HR	Y	in-h	error	no	DPA	Y	Current
	INF, GSV, HCS	? pro RH	pro	on, off, HR	NDL	TP	both	no	DPA	Y	Current
	INF, GSV, HCS	?	cont	on, off, HR	NDL	TP	both	no	DPA	Y	Current
	CSV, CSF	Cn HR, pro	pro	on, HR	NDL	in-h	both	OPA	DPA	Y	Current
	EIP, GST, OGS	C, HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	CSV, CSF, AGC	C, pro	pro	on, off, MP	Y	in-h	FTC	no	DPA	Y	Current
	FNS, MED, INS	C RH	cont	HR, MP	AUR	in-h	both	no	DPA	Y	Current
	ADV	C	cont	on	Y	in-h	FTC	BBB, NAI, OPA	BBB, NAI, OPA	no	Current
	MED	C	cont	on	NDL	TP	FTC	TRUSTe	TRUSTe	no	Current
	BOK	C	cont	on, off, MP	Y	in-h	FTC	no	BBB	no	Current
	OGS	HR	cont	on, off, HR, MP	NDL	in-h	both	no	DPA	Y	Current
	GFT, APP, ARW	C	cont	on, off, MP	Y	in-h	FTC	BBB	BBBOnL	no	Current
	ELC, BTC	C, HR, RE	cont	on, HR, MP	No	in-h	both	no	DPA	Y	Current
	ADV, CSF	C	cont	on	Y	in-h	FTC	TRUSTe, CAUCE	no	Y	Current
	ADV, CSF, INF	C, pro	pro	on, off	Y	in-h	FTC	no	DPA	Y	Current
	TRA	C	cont	on, off	No	in-h	FTC	no	DMA	no	Current
	CSF, CSV	HR	cont	HR	PA	in-h	error	no	DPA	Y	Current
	CSV	C, RH	cont	on	NDL	in-h	FTC	no	DPA	Y	Current
	CSF, CSV, GSV	C	cont	on	NDL	in-h TI	FTC	TRUSTe	TRUSTe	no	Current
	CSF, INF	C, RE, pro	pro	on, off, MP	NDL	in-h TI	FTC	no	DPA	Y	Current
	CSF, CSV	?	cont	on	Y	in-h TI	FTC	TRUSTe	TRUSTe	no	Current
	GSV	RE RH	cont	on, off, HR	Y	TP	both	TRUSTe	TRUSTe	Y	Current
	ACT	HR	cont	HR	NDL	in-h	both	DoC	OR	Y	Current
	EDS, CSV	C RH	cont	on	Y	in-h	both	TRUSTe	TRUSTe	Y	Current
	HCS	C RH, M	cont	on, off, HR	Y	in-h	both	TRUSTe	TRUSTe, DPA	Y	Current
	INV, FNS	HR	cont	HR	NDL	in-h	error	no	DPA	Y	Current
	GSV	HR	cont	HR, MP	NDL	in-h	error	no	DPA	Y	Current
	CON, PAP, PUL	HR	cont	HR	N	in-h	error	GHEI	DPA	Y	Current
	EDS, MCS, EMP	C	cont	on	NDL	in-h	FTC	BBB	BBB	no	Current
	TES, EDS	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	CSV	C	cont	on	No	TP	FTC	TRUSTe	TRUSTe	no	Not
	GCG, FOD	HR	cont	on, off, HR, MP	PA	in-h	both	no	DPA	Y	Current
	ADV	C	cont	on, off	NDL	in-h	FTC	no	DMA	no	Current
	GSV	RE	cont	on, off, MP	Y	in-h	FTC	no	DPA	Y	Not
	TRA	T	cont	on, off, HR	NDL	in-h	FTC	no	WWTS, DPA	Y	Not
	TRA	T	cont	on, off, MP	NDL	in-h	FTC	no	DPA	Y	Current

	GSV, TXP, DRG	HR	cont	HR	Intranet	in-h	error	no	DPA	Y	Current
	TRA	HR, T	cont	on, off, HR	AUR	in-h	both	no	DPA	Y	Current
	ADV	C, RH	cont	on, HR	NDL	in-h	both	no	DPA	Y	Not
	CSV, INF	C, pro	pro	on, off, MP	No	TP	FTC	TRUSTe	TRUSTe	no	Current
	INF	C, pro	pro	on, off, MP	NDL	in-h	FTC	no	DPA	Y	Current
	CSF, FNS	C, pro	pro	on	Y	in-h	FTC	TRUSTe	TRUSTe	Y	Current
	MUS	C	cont	on	NDL	in-h	FTC	no	DPA	Y	Current
	CSV, TES, CSF	C	cont	on	NDL	in-h	FTC	no	DPA	Y	Current
	CSV	C	cont	on	Y	TP	FTC	TRUSTe	TRUSTe	no	Current
	CSF, CSV	C	cont	on	Y	TP	FTC	BBB	BBB	no	Current

Cellule: B1
Commentaire: Veronica:
Industry Sector:
ACE: Architectural/Construction/Eng Svc
ACR: Air Conditioning & Refrigeration Eq.
ACT: Accounting Services
ADV: Advertising Services
AGC: Agricultural Chemicals
AGM: Agricultural Machinery & Equipment
AIR: Aircraft and Parts
APP: Apparel
APS: Automotive Parts & Service Equipment
ARW: Artwork
AUT: Automoviles & Light Trucks/vans
AUV: Audio/Visual Equipment
AVS: Aviation Services
BOK: Books & Periodicals
BTC: Biotechnology
BUS: Business Equipment (other than computers)
CEL: Consumer Electronics
COL: Coal
CON: Construction Equipment
COS: Cosmetics & Toiletries
CPT: Computer & Peripherals
CRM: Ceramics Fine Advanced
CSF: Computer Software
CSV: Computer Services
DFN: Defense Industry Equipment
DRG: Drugs and Pharmaceuticals
EDS: Education and Training
EIP: Electronic Industry Prod/Test
ELC: Electronic Components
ELP: Electrical Power Systems
EMP: Employment Services
FLM: Films Videos & Other Recording
FNS: Financial Services
FOD: Foods Processed

FOT: Footwear
GCG: General Consumer Goods
GFT: Giftware
GIE: General Industrial Equipment & Supplies
GST: General Science and Technology
GSV: General Services
HCG: Hosehold Consumer Goods
HCS: Health Care Services
ICH: Industrial Chemicals
INF: Information Services
INS: Insurance Services
INV: Investment Services
LAB: Laboratory Scientific Instruments
LES: Leasing Services
MCS: Management Consulting Services
MED: Medical Equipment
MTL: Machine Tools & Metal Working Equipment
MUS: Musical Instruments
OGM: Oil & Gas Field Machinery
OGS: Oil Gas Mineral Production/Exp Srv
OMS: Operations & Maintenance Services
PAP: Paper & Paperboard
PCI: Process Controls Industrial
PHT: Photographic Equipment
PMR: Plastic Materials & Resin
PRT: Port & Shipbuilding Equipment
PUL: Pulp & Paper Machinery
PVC: Pumps Valves & Compressors
REQ: Renewable Energy Equipment
RRE: Railroad Equipment
SPT: Sporting Goods Recreatinal Equipment
TEL: Telecommunication Equipment
TES: Telecommunications Services
TOY: Toy & Games
TRA: Travel and Tourism Services
TRK: Trucks, Trailers & Buses
TRN: Transportation Services (Except Aviation)

TXF: Textile Fabrics

Cellule: I7
Commentaire: HON: Healthcare on the Net
and TRUSTe's privacy guidelines

Cellule: I15
Commentaire: BBBOnLine Privacy Seal Program

Cellule: I18
Commentaire: CASRO: Council of American Survey Research Organizations

Cellule: C20
Commentaire: The following note is included in the item "Personal information received from the EU": "Not applicable. We do not process personal information. Data we work with relates to real state, including location, physical property attributes, and sales prices".

Cellule: I21
Commentaire: AAA: American Arbitration Association

Cellule: I51
Commentaire: Special International BNI Task Force for Data Privacy Issues

Cellule: I54
Commentaire: Greater Boston Chamber of Commerce

Cellule: I63
Commentaire: DMA Safe Harbour Program, TRUSTe

Cellule: C64
Commentaire: Assistance with insurance realted disputes.

Cellule: C93
Commentaire: not clear what is the data received

Cellule: I102

Commentaire: CASRO, Marketing Reasearch Association, ESOMAR (?), and TRUSTe

Cellule: I105
Commentaire: TRUSTe, DMA SHP, Association ofr Interactive Marketing Council for Responsinle E-mail, NAI's E-mail Service Provide Coalitin

Cellule: I122
Commentaire: Entertainment Software Ratings Board Privacy Online Program

Cellule: J126
Commentaire: "Exception for third party enforcement body".

Cellule: I149
Commentaire: American Association of Blood Banks (AABB). The DNA accreditation committee in charge of immigration and naturalization.

Cellule: C150
Commentaire: They do not specify what kind of data they process

Cellule: J153
Commentaire: Judicial Arbitration and Mediation Service

Cellule: I155
Commentaire: They are working on meeting HIPPA regulaions

Cellule: I172
Commentaire: Part of the Secure Site Network certified by Verisign, Inc., a licensee of the TRUSTe Privacy Program.

Cellule: I175
Commentaire: 1)European Privacy Officers Network
2)European Privacy Officers Forum
3)IAPO
4)Society for Human Resources Management
5)Center for Legal and Social Responsibility
PRIVACY PROGRAM???

Cellule: I188
Commentaire: North Alabama International Trade Association

Cellule: C202
Commentaire:
They represent the following: "X does not currently receive personal information from the EU,it has no activities with respect to such information"

Cellule: I206
Commentaire: Privacy and American Business; The Privacy Council

Cellule: I214
Commentaire: CASRO & MRA (Marketing Research Association)

Cellule: I219
Commentaire: Privacy & American Business, International Organization of Privacy Officers, EPON

Cellule: I225
Commentaire: DMA, but we can't say that HIPPA, COPPA

Cellule: I228
Commentaire: CASRO, ESOMAR, MRA

Cellule: I264
Commentaire: IAPP International Association of Privacy Officers

Cellule: I270
Commentaire: TRUSTe PrivAcy Bot

Cellule: I273
Commentaire: American Society for Insdustrial Security's Privacy and Personal Information Management Council

Cellule: I288
Commentaire: "We comply with the P3P... CNIL Memeber. We registeed our privacy policy to the Commission Nationale de l'Informatique et des Libertés. HON Member. We comply with the HON Code of Conduct..."

Cellule: I312

Commentaire: TRUSTe, CAUCE, and the Direct Marketing Association Council for Responsible E-mail

Cellule: I326
Commentaire: Montly UK TPS TPS file subscription

Cellule: C335
Commentaire: Name, address and charitable donation history from a response handling company in the United Kingdom is transmitted to the US and stored as a data base by client.

Cellule: I338
Commentaire: The Code of Federal Regulations, The Belmont Report, The Department of Health and Human Services Federalwide Assurance Protection for Human Subjects

Cellule: I349
Commentaire:
Recipient of KPMG Security Seal as a result of regulatory scheduled security audits; member of Chemical Industry Data Exchange (CIDX) Cyber Security Practices, Standards & Technology Initiative

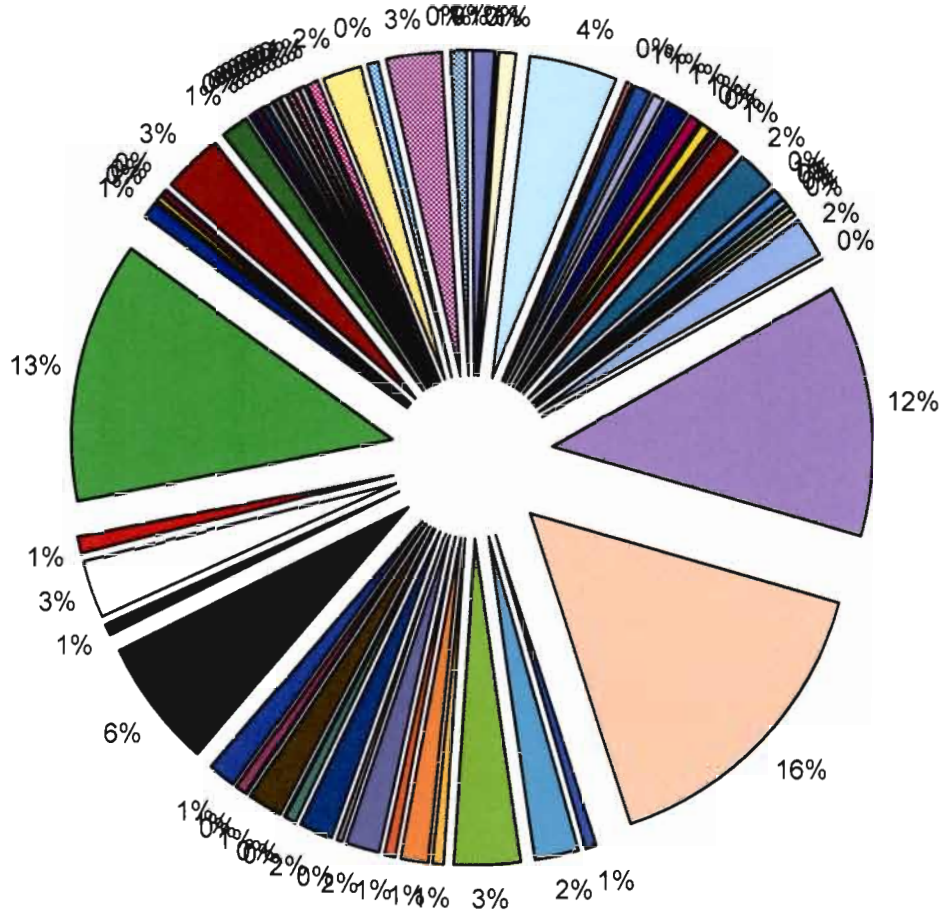
Cellule: I360
Commentaire: Online Privacy Alliance

Cellule: I379
Commentaire:
US Department of Commerce Safe Harbour Program

Cellule: J379
Commentaire: On-Line resolution www.onlineresolution.com

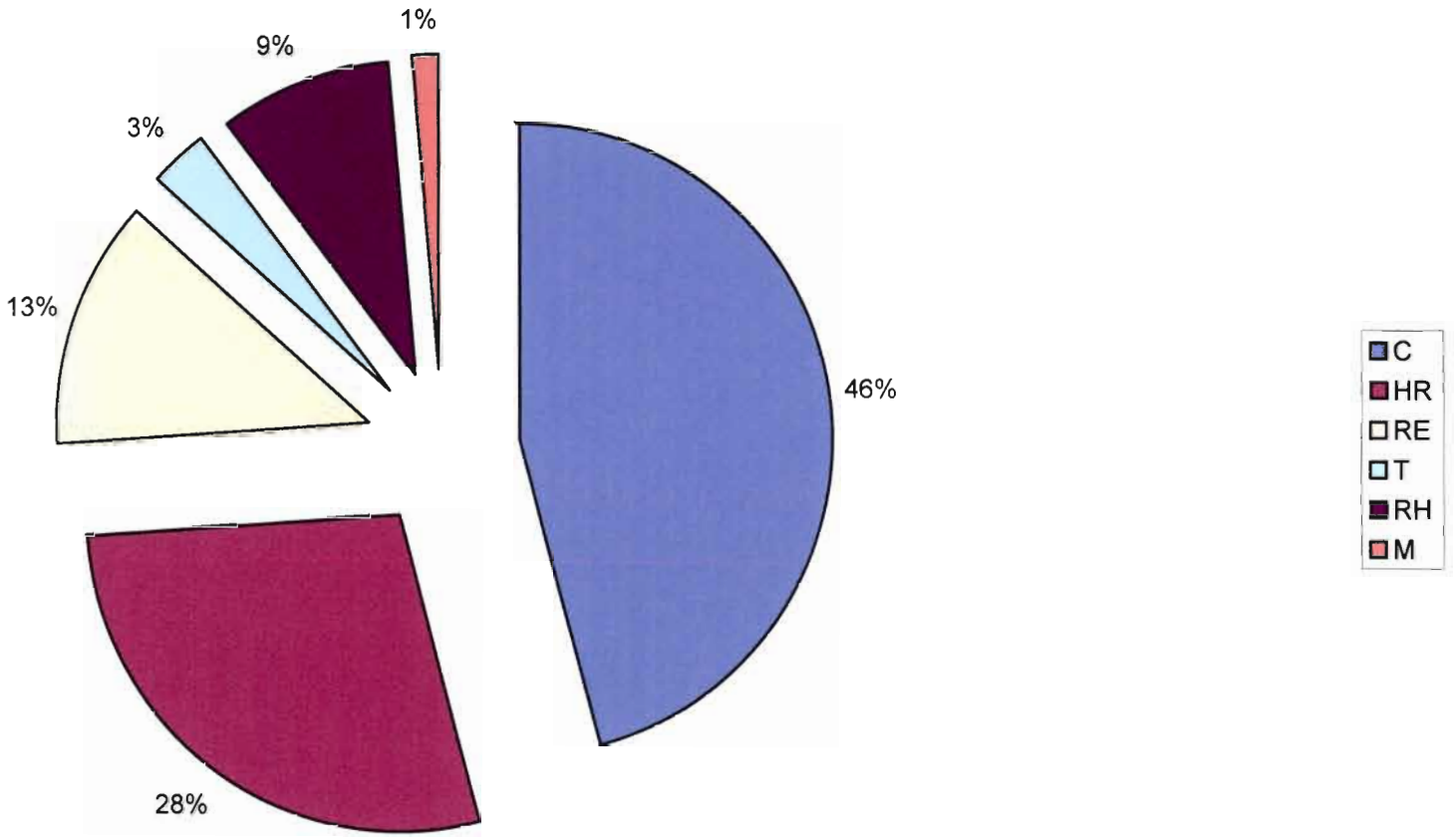
Cellule: I384
Commentaire: Guidelines for Handling Employee Information.

Cellule: J391
Commentaire: Safe Harbour Team at World Wide Travel Service

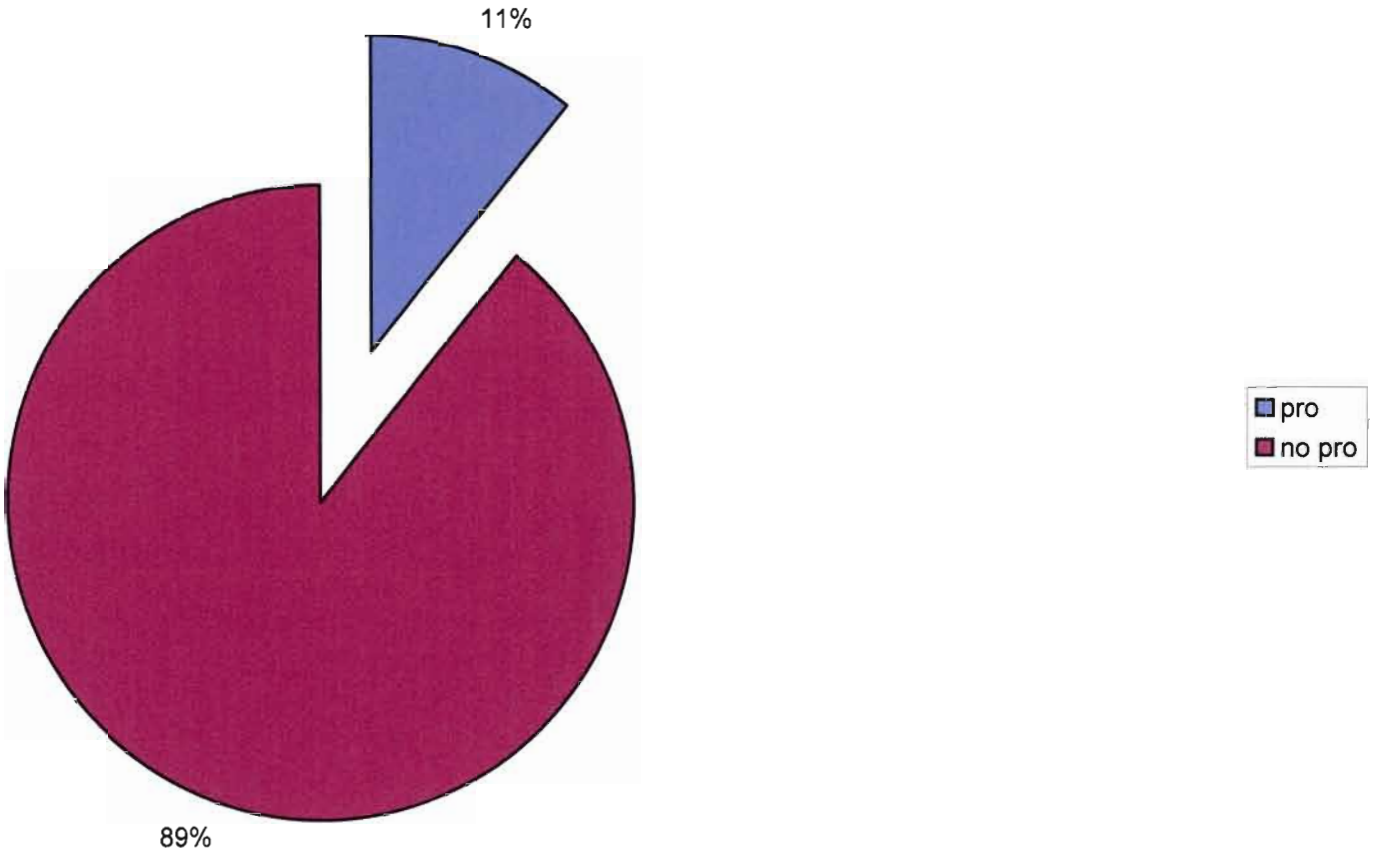


ACE ACR ACT ADV AGC AGM AIR APP APS
ARW AUT AUV AVS BOK BTC BUS CEL COL
CON COS CPT CRM CSF CSV DFN DRG EDS
EIP ELC ELP EMP FLM FNS FOD FOT GCG
GFT GIE GST GSV HCG HCS ICH INF INS
INV LAB LES MCS MED MTL MUS OGM OGS
OMS PAP PCI PHT PMR PRT PUL PVC REQ
RRE SPT TEL TES TOY TRA TRK TRN TXF

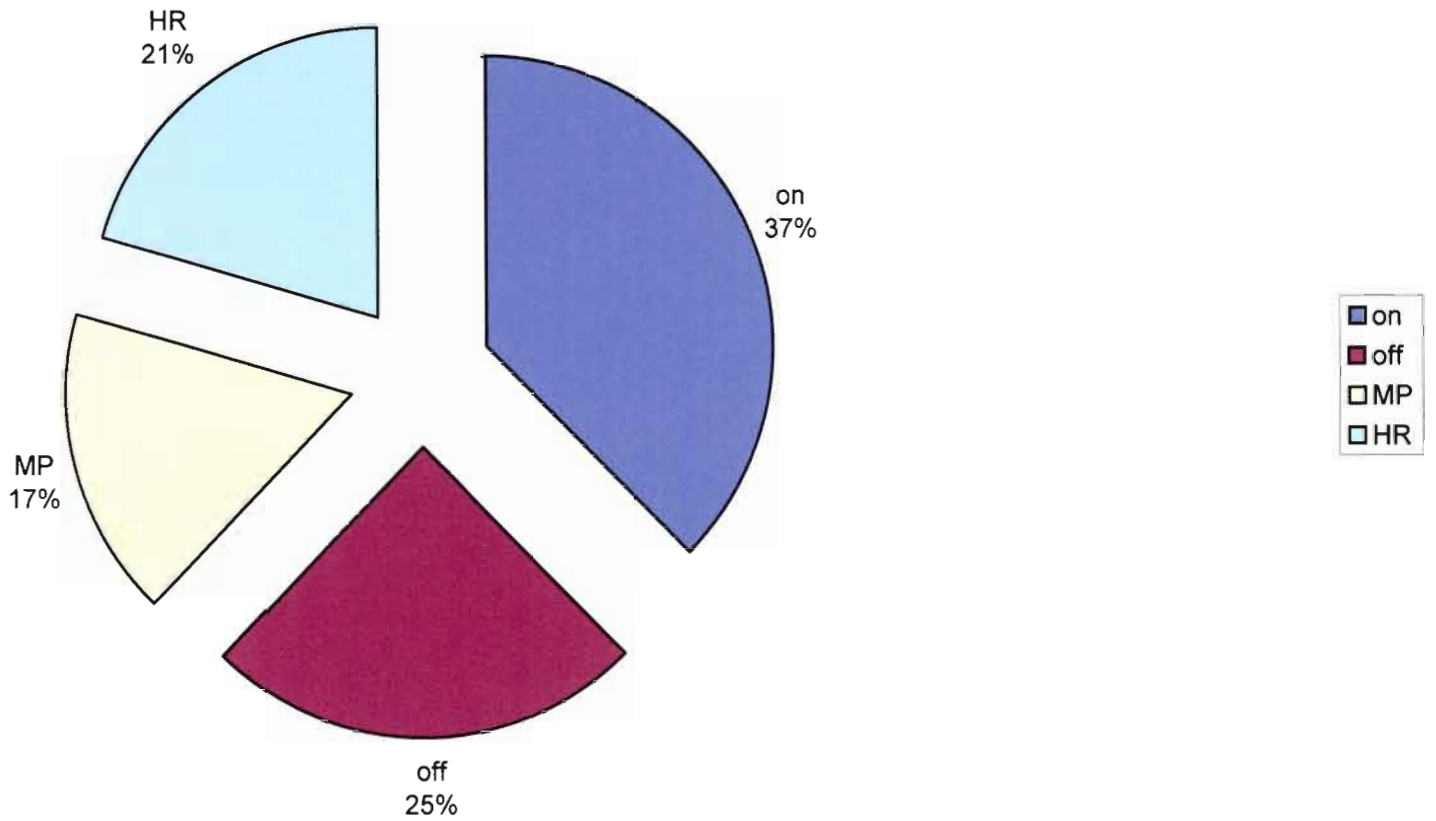
Data type



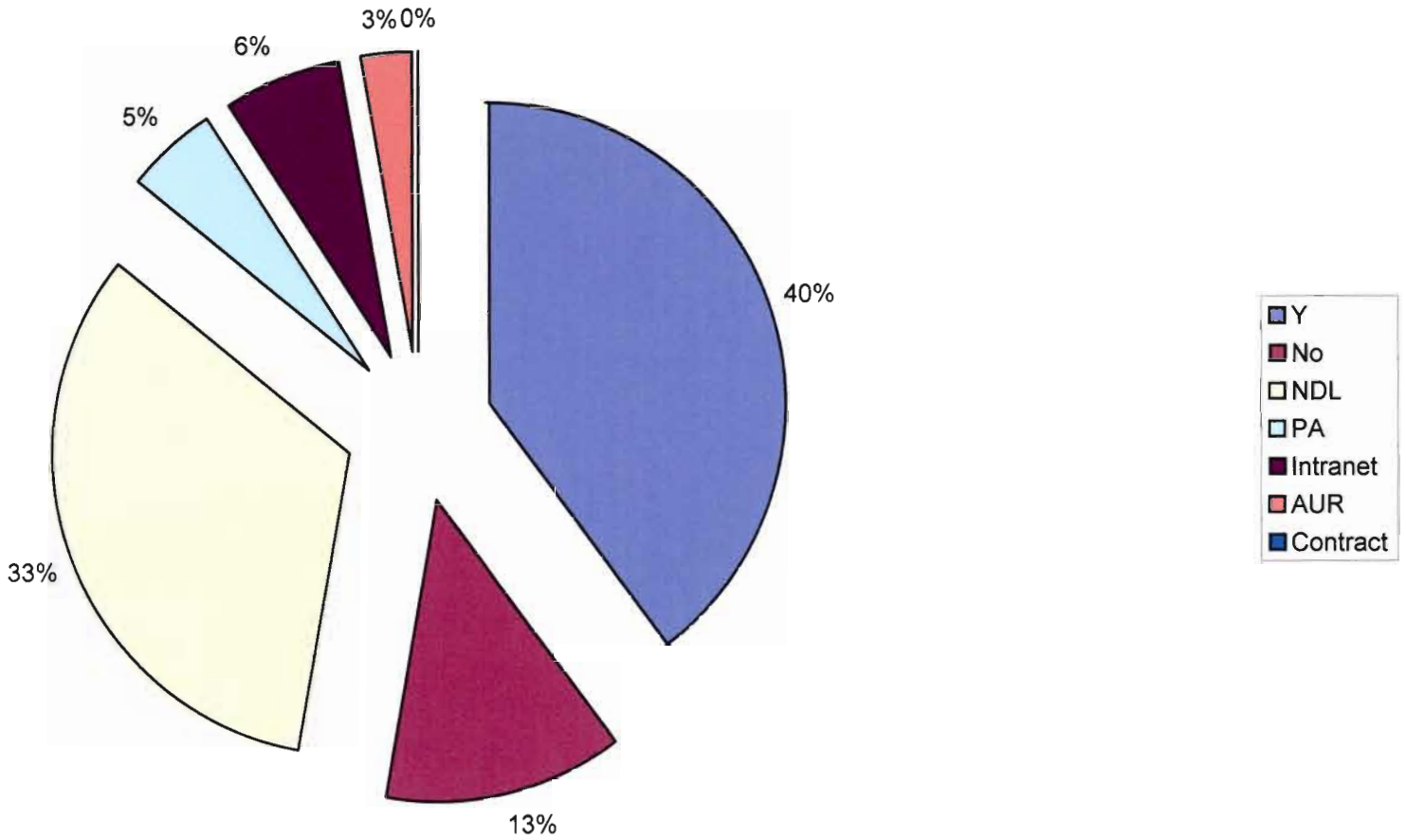
Pro / no Pro



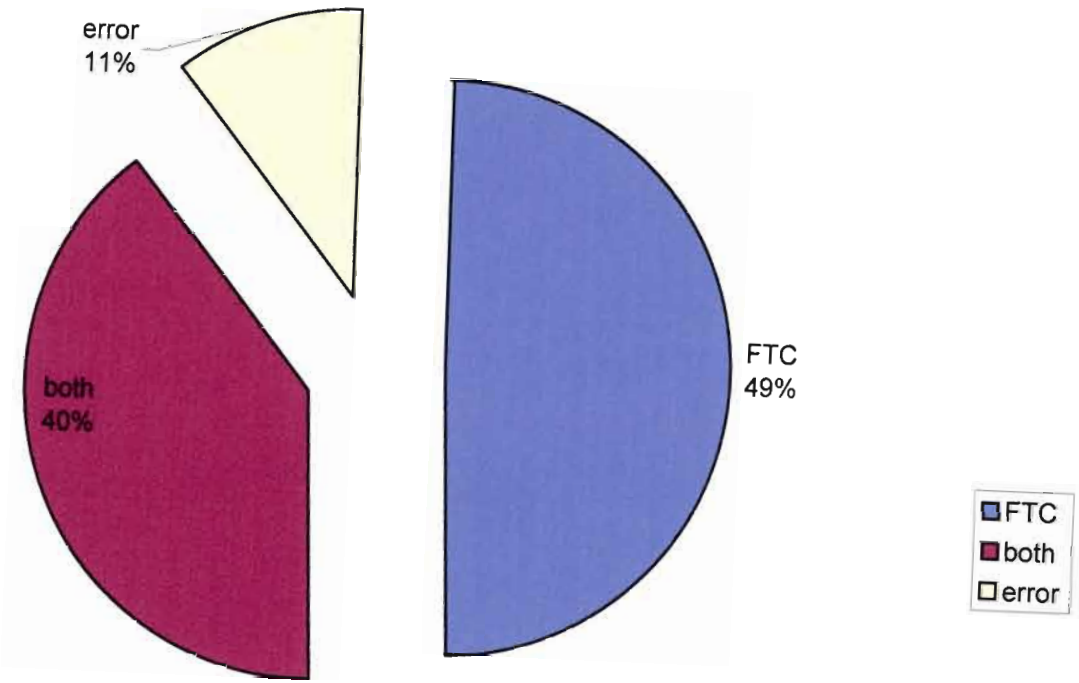
Personal Data Covered

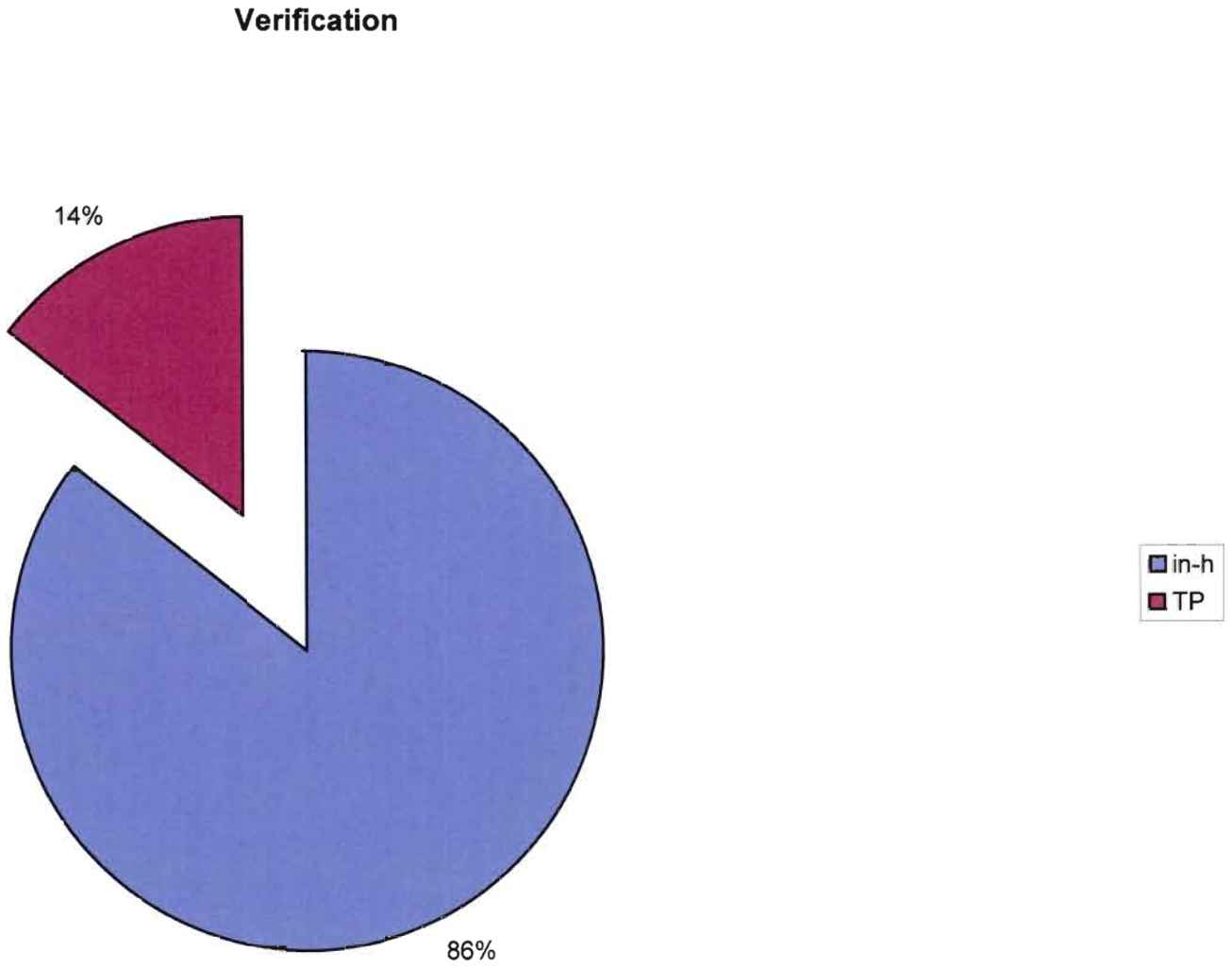


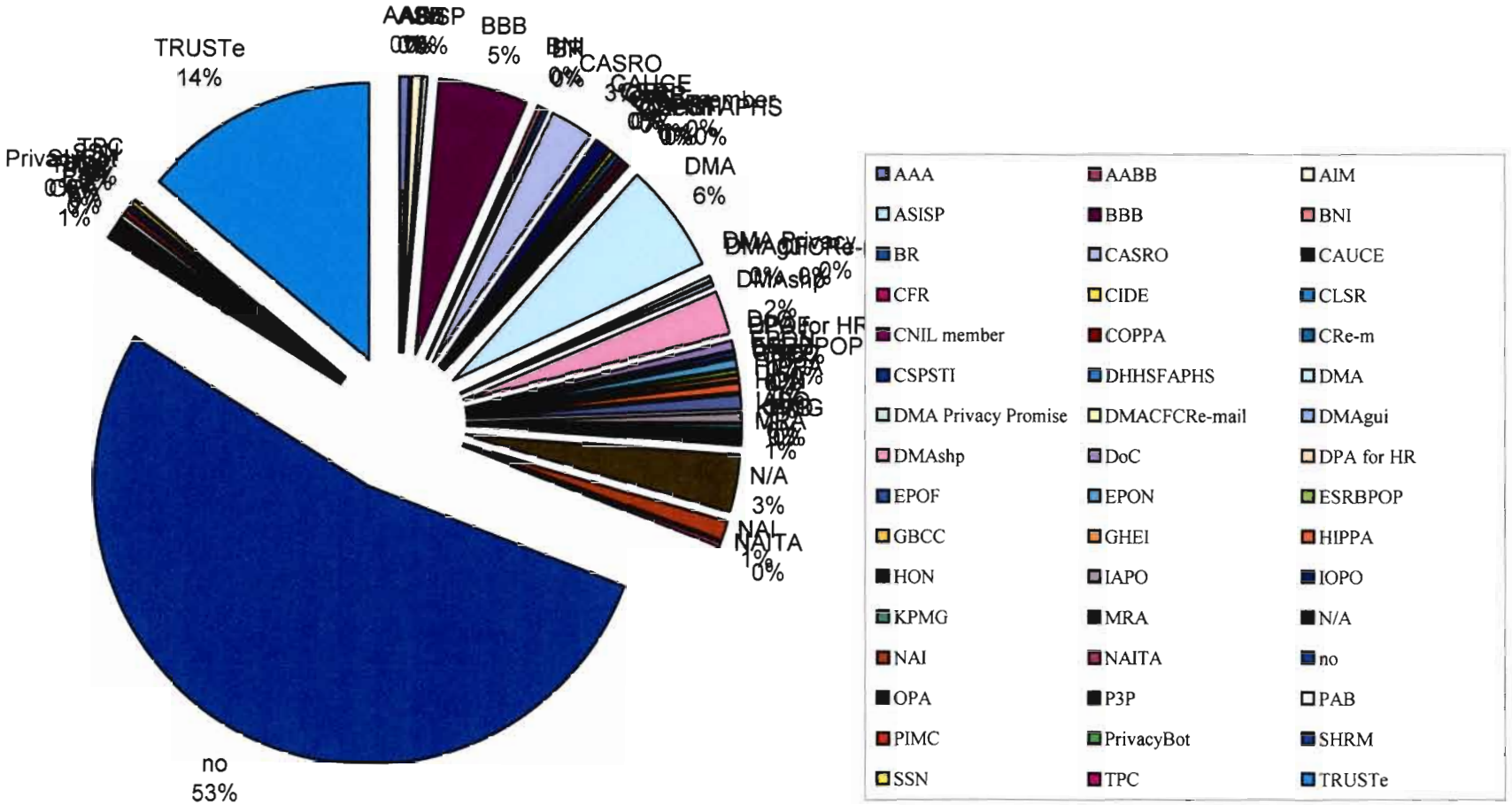
Accurate Location

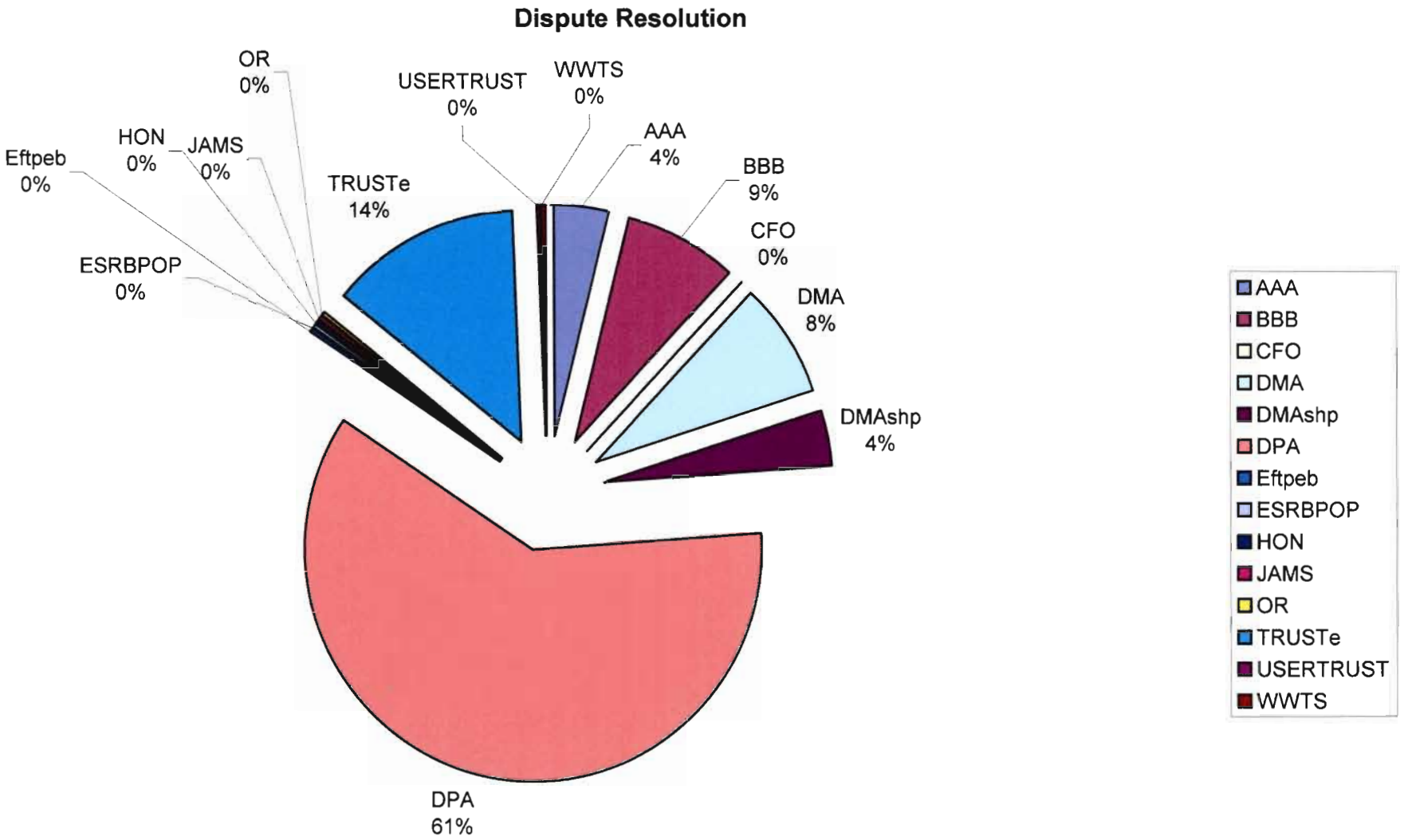


Regulated by

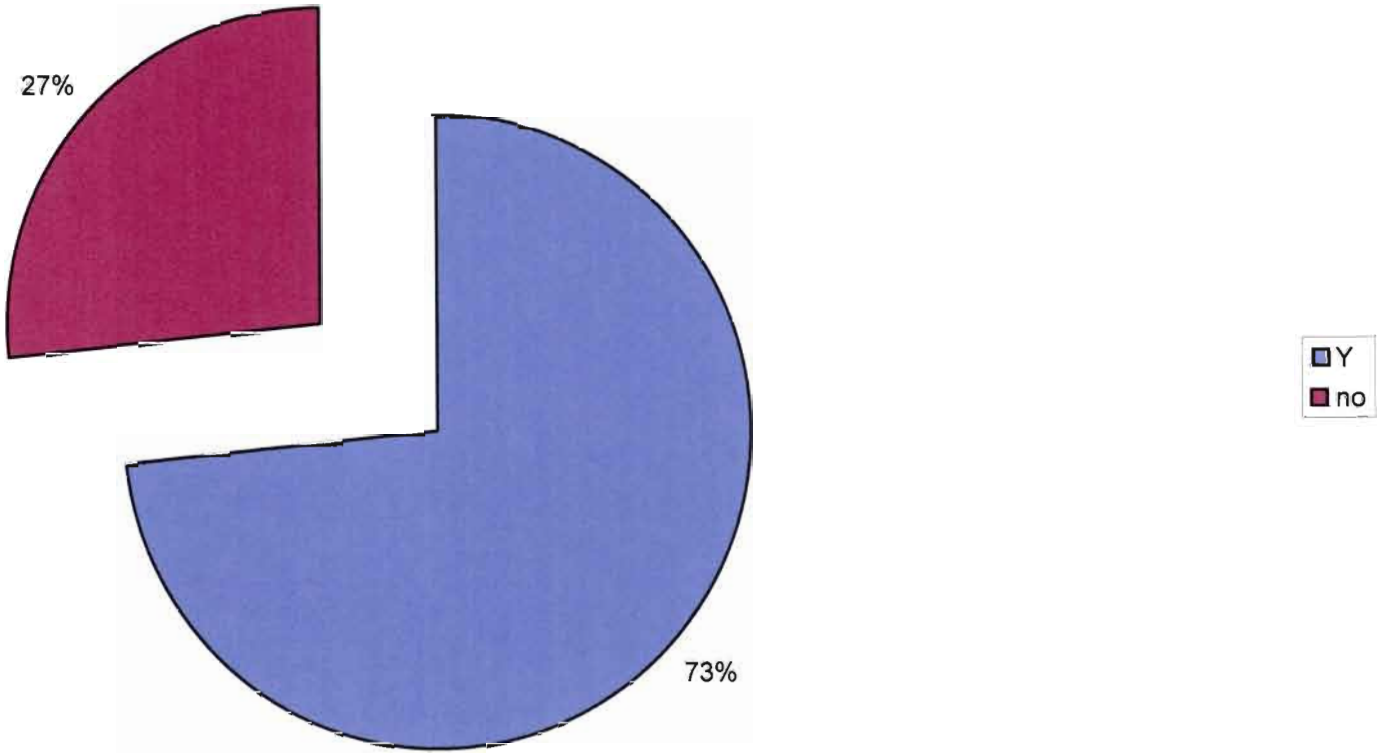



Verification
14%
86%
in-h
TP

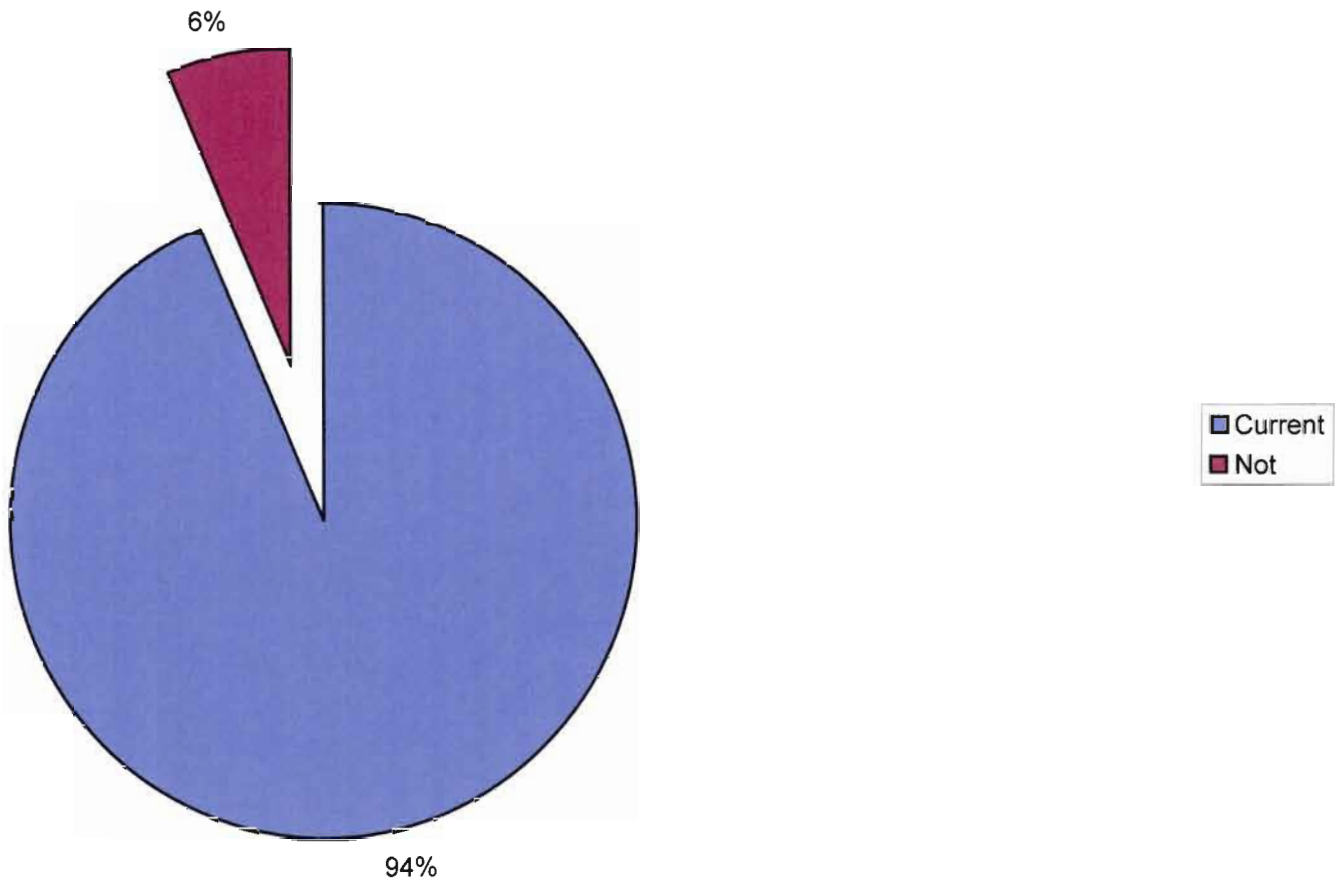

TRUSTe
14%
BBB
5%
CASRO
DMA
6%
N/A
3%
no
53%
AAA
AABB
AIM
ASISP
BBB
BNI
BR
CASRO
CAUCE
CFR
CIDE
CLSR
CNIL member
COPPA
CRe-m
CSPSTI
DHHSFAPHS
DMA
DMA Privacy Promise
DMACFCRe-mail
DMAgui
DMAshp
DoC
DPA for HR
EPOF
EPON
ESRBPOP
GBCC
GHEI
HIPPA
HON
IAPO
IOPO
KPMG
MRA
N/A
NAI
NAITA
no
OPA
P3P
PAB
PIMC
PrivacyBot
SHRM
SSN
TPC
TRUSTe


Dispute Resolution
OR 0%
USERTRUST 0%
WWTS 0%
AAA 4%
BBB 9%
CFO 0%
DMA 8%
DMAshp 4%
DPA 61%
Eftpeb 0%
HON 0%
JAMS 0%
TRUSTe 14%
ESRBPOP 0%
AAA
BBB
CFO
DMA
DMAshp
DPA
Eftpeb
ESRBPOP
HON
JAMS
OR
TRUSTe
USERTRUST
WWTS

Cooperation DPA

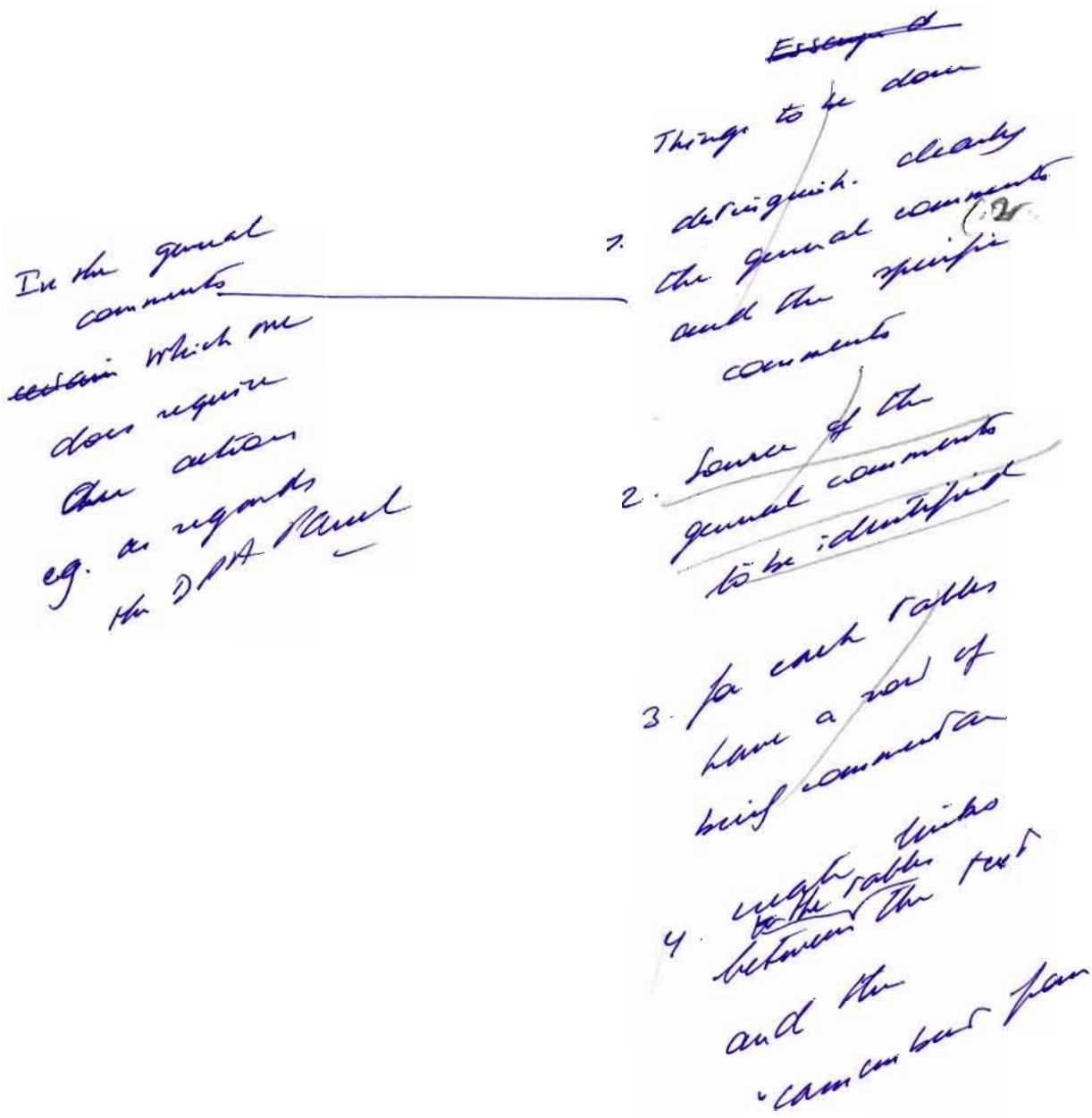


Certification



APPENDIX VI

Data Tables and Graphics of Point 3.1 (Visible compliance/implementation)



	A	B	C	D	E	F	G	H	I
1	**Table 1.1: SH Company Eligibility for Safe Harbor (as of November 3, 2003)**								
2	*Company*		*Public Disclosure of Privacy Policy*	*Printable Policy*	*Jurisdiction (FTC/DOT)*	*Coverage*	*Policy Applies to EU Data Indefinitely*	*Policy Signals US Law Preventing Compliance*	*Cont / pro*
3	1		yes	yes	FTC	Limited no HR	no	no	controller
4	2		Intranet	unknown	error	Limited - HR	Unknown	Unknown	controller
5	3		yes	yes	FTC	Limited no HR	no	no	cont/ proc
6	4		no	unknown	FTC	Limited	Unknown	Unknown	processor
7	5		Intranet	unknown	error	Limited - HR	Unknown	Unknown	controller
8	6		yes	yes	FTC	Limited no HR	yes	no	controller
9	7		yes/no	yes/no	FTC, error	Limited, no off	unknown	unknown	cont/ proc
10	8		Physical address	unknown	FTC	Limited no HR/on	unknown	unknown	processor
11	9		yes/no	yes/no	FTC, error	Unlimited	yes	no	controller
12	10		yes	yes	FTC	Limited - on	no	no	controller
13	11		yes	yes	FTC	Limited - on	yes	no	controller
14	12		yes	yes	FTC	Limited - on	no	no	controller
15	13		yes/no	yes/no	FTC & error	Limited - HR/on	no	no	controller
16	14		yes/no	yes/no	FTC, error	Unlimited	no	no	controller
17	15		yes/no	yes/no	FTC	Limited no HR	no	no	controller
18	16		yes	yes	FTC	Limited no HR	yes	no	processor
19	17		yes	yes	FTC & error	Limited no off	no	no	controller
20	18		no	unknown	FTC & error	Limited - HR	Unknown	Unknown	controller
21	19		Intranet	yes	FTC & error	unclear	no	no	controller
22	20		yes	yes	FTC	Limited no HR	no	no	controller
23	21		no	unknown	FTC	Limited no HR	unknown	unknown	processor
24	22		yes/no	yes/no	FTC, error	Unlimited	no	no	controller
25	23		no	no	FTC	Limited no HR	no	no	controller
26	24		yes	yes	FTC	Limited no HR	no	no	controller
27	25		no	unknown	FTC	Limited no HR	unknown	unknown	controller
28	26		yes/no	yes/no	FTC, error	Unlimited	no	no	controller
29	27		Intranet	yes	error	Limited - HR	no	no	controller
30	28		phsysical address	unknown	error	Limited - HR	unknown	unknown	controller
31	29		no	unknown	FTC	Limited no HR	unknown	no	controller
32	30		yes	yes	error	Limited - HR	no	no	controller
33	31		yes	yes	error	Limited - HR	no	no	controller
34	32		Intranet	unknown	FTC	Limited - no HR	unknown	unknown	processor
35	33		yes	yes	FTC	Limited - no HR	yes	no	processor
36	34		physical address	yes	error	Limited - HR	yes	no	controller
37	35		yes	yes	FTC	Limited - no HR	no	no	controller
38	36		yes	yes	FTC	Limited - no HR	no	no	controller
39	37		yes	yes	FTC, error	Unlimited	yes	no	processor
40	38		yes	yes	FTC	Limited - no HR	no	no	controller
41	39		yes	yes	error	Limited - HR	no	no	controller
42	40		yes	yes	FTC	Limited - no HR	yes	no	controller
43	41		yes	yes	FTC	Limited - no HR	no	no	controller

Cellule: C2
Commentaire: Recital 5; Art. 2(a). If a policy is not publicly disclosed, there is not likely to be any basis for a deceptive practice that would trigger the FTC's jurisdiction.

Cellule: D2
Commentaire: This is necessary for data subjects, data exporters and DPAs to be able to evaluate a privacy policy at a specific moment in time.

Cellule: E2
Commentaire: SH Art. 1(2)(b). For the FTC to have jurisdiction, a company must publicly post a privacy policy.

Cellule: F2
Commentaire: Organizations may subscribe to the Safe Harbor for the treatment of all their EU-origin data or for only some of their EU-origin data.

Cellule: G2
Commentaire: FAQ 6 states that "the undertaking to adhere to the SH Principles is not time-limited .... [the] undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them , even if it subsequently leaves SH."

Cellule: G3
Commentaire: The company reserves the right to change the policy

Cellule: C4
Commentaire:
The privacy Policy covers data collected in the operation of the website, but the personal data covered, as declaraed in the self-certification formulaire, is only HR data

Cellule: D4
Commentaire: The privacy Policy covers data collected in the operation of the website, but the personal data covered, as declaraed in the self-certification formulaire, is only HR data

Cellule: E4
Commentaire: Error in certification letter, the FTC has no jurisdiction over HR data,

Cellule: H5
Commentaire: only a general statement concening disclosure to law enforcement.

Cellule: D7
Commentaire: Through the homepage it is possible to access to a privacy policy that covers data collected on the Internet, but not HR data

Cellule: C9
Commentaire:

Yes: the Privacy Policy describes the company as only processor,and they made representations concerning the data they receive as processors.
No: however, in the certification page they represent to cover also HR data, and they do not mention where the privacy policy for HR data is available, they do not publicly disclosed it's location.
In this privacy policy a doble analysis should be made. One concerning the processor transfer,where all the SH principles, except the security one should be answered as "not applicable"; and a second one concerning HR data where, considering that we don't have access to the privacy policy all the answeres should be "unknown".
However, the company will be scored "unknown" where relevant because the SH concerns in general obligations for data controllers.

Cellule: C10
Commentaire:
Corp. Ofc. Also available via e-mail

Cellule: C11
Commentaire:
The privacy Policy covers data collected in the operation of the website, but the personal data covered, as declaraed in the self-certification formulaire, is also HR data, off-line and manually processed.
The analysis is made on the printed privacy policy.

Cellule: C16
Commentaire:
on-off-MP and HR, however the policy covers only on-line data

Cellule: C17
Commentaire:
on-off-manually processed. However, the policy covers only on-line data

Cellule: C21
Commentaire:
The company was contacted in order to ask for the privacy policy since the link given is of an Intranet. The policy reveived by e-mail does not only cover HR data but also consumer's data, so, the availability on an Intranet is not enough.

Cellule: F21
Commentaire: "personal data covered: all personal data"? Then, the description of the information received from the EU is not clear

Cellule: C24

Commentaire: The policy only covers on-line collected data, but the cetification page represents to import also manually processed and human resources data

Cellule: C31
Commentaire: Certifycation page says off-line and manually pocessed data, while publicly available policy concerns on-line data.

Cellule: F35
Commentaire: neither the certification page, nor the security policy specify this, we only know that (the comapany) processes data for health care services purposes

Cellule: C36
Commentaire: fysical address (contact organization)

	A	C	D	E	F	G	H	I	J
1	**Table 1.2: SH Company Eligibility for Safe Harbor (FAQ 6 Certification) (as of November 3, 2003)**								
2	*Company*	*Name Reported*	*Address Reported*	*Email*	*Tel*	*Fax*	*Description of Types of Processed EU Data*	*Public Location of Policy Provided*	*Accurate Location*
3	1	yes	yes	yes	yes	yes	unclear	yes	yes
4	2	yes	yes	yes	yes	yes	yes	Intranet	Unknown
5	3	yes	yes	yes	yes	yes	unclear	yes	yes
6	4	yes	yes	yes	yes	yes	yes	no	no
7	5	yes	yes	yes	yes	yes	yes	Intranet	Unknown
8	6	yes	yes	yes	yes	yes	yes	yes	yes
9	7	yes	yes	yes	yes	yes	yes	yes/no	yes/no
10	8	yes	yes	yes	yes	yes	no	Physical address	unknown
11	9	yes	yes	yes	yes	yes	yes	yes/no	no
12	10	yes	yes	yes	yes	yes	unclear	yes	no
13	11	yes	yes	yes	yes	yes	yes	yes	yes
14	12	yes	yes	yes	yes	yes	no	yes	no
15	13	yes	yes	yes	yes	yes	yes	yes/no	yes/no
16	14	yes	yes	yes	yes	yes	no	yes/no	no
17	15	yes	yes	yes	yes	yes	no	yes/no	no
18	16	yes	yes	yes	yes	yes	no	yes	yes
19	17	yes	yes	yes	yes	yes	unclear	yes	no
20	18	yes	yes	yes	yes	yes	unclear	no	no
21	19	yes	yes	yes	yes	yes	unclear	Intranet	unknown
22	20	yes	yes	yes	yes	yes	yes	yes	no
23	21	yes	yes	yes	yes	yes	no	no	Unknown
24	22	yes	yes	yes	yes	yes	yes	yes/no	yes/no
25	23	yes	yes	yes	yes	yes	unclear	no	no
26	24	yes	yes	yes	yes	yes	no	yes	yes
27	25	yes	yes	yes	yes	yes	unknown	no	Unknown
28	26	yes	yes	yes	yes	no	no	yes/no	yes/no
29	27	yes	yes	yes	yes	yes	yes	Intranet	unknown
30	28	yes	yes	yes	yes	yes	yes	Physical address	unknown
31	29	yes	yes	yes	yes	yes	yes	no	no
32	30	yes	yes	yes	yes	yes	yes	yes	no
33	31	yes	yes	yes	yes	yes	yes	yes	yes
34	32	yes	yes	yes	yes	yes	unclear	Intranet	unknown
35	33	yes	yes	yes	yes	yes	no	yes	unknown
36	34	yes	yes	yes	yes	yes	yes	Physical address	yes
37	35	yes	yes	yes	yes	yes	no	yes	yes
38	36	yes	yes	yes	yes	yes	no	yes	yes
39	37	yes	yes	yes	yes	yes	yes	yes	no
40	38	yes	yes	yes	yes	yes	no	yes	yes
41	39	yes	yes	yes	yes	yes	no	yes	yes
42	40	yes	yes	yes	yes	yes	no	yes	no
43	41	yes	yes	yes	yes	yes	yes	yes	yes

Cellule: E2
Commentaire: This criteria indicates if the Certification lists either a general organizational email address or a specific contact email address for Safe Harbor issues.

Cellule: H2
Commentaire: FAQ 6 requires that the certification include a "description of the activities of the organization with respect to personal information received from the EU."

Cellule: I2
Commentaire: FAQ 6 requires the organization to state "where the privacy policy is available for viewing by the public."

Cellule: J2
Commentaire: This indicates if the address shown on the Certification is an accurate and precise location for the privacy policy. When the Certification indicates a web site that is not the actual page for the privacy policy, the location will be marked as inaccurate.

Cellule: I5
Commentaire: But the Policy is difficult to find if one starts from the Home Page, there's no direct reference to it there

	A	B	C	D	E	F	G	H	I	J	K
1	**Table 1.3: SH Company Eligibility for Safe Harbor (FAQ 6 Certification) (as of November 3, 2003)**										
2	*Company*		*Date of SH Certification*	*Policy Effective Date*	*Contact Office*	*Regulatory Agency*	*Privacy Program Membership*	*Verification Method*	*Independent Recourse Mechanism*	*HR Data*	*EU DPA Coop*
3	1		8/12/2002	1/12/2002	yes	yes	no	In-house	DPA	no	yes
4	2		25/02/2002	2/01/2002	yes	no	Unknown	In-house	DPA	yes	yes
5	3		18/08/2003	19/08/2003	yes	yes	AAA	In-house	AAA	no	no
6	4		27/11/2002	janv-02	yes	yes	DMA	In-house	DMAshp	no	no
7	5		24/05/2002	1/05/2002	yes	no	no	In-house	DPA	yes	yes
8	6		6/03/2002	March 2002	yes	yes	no	In-house	DPA	no	yes
9	7		27/01/2001	2/09/2001	yes	yes/no	BBB	In-house	BBB & DPA	yes	yes
10	8		9/04/2004	7/04/2003	yes	yes	no	in-house	BBB	no	no
11	9		20/09/2004	07/18/2002	yes	yes/no	no	in-house	DPA	yes	yes
12	10		7/01/2003	26/07/2001	yes	yes	TRUSTe	in-house	TRUSTe & BBB	no	no
13	11		3/07/2002	1/07/2002	yes	yes	no	In-house	DPA	no	yes
14	12		15/01/2002	1/01/2002	yes	yes	no	TP	DPA	no	yes
15	13		6/03/2003	12/01/2000	yes	yes/no	no	in-house	DPA & AAA	yes	yes
16	14		15/01/2002	2/04/2002	yes	yes/no	no	in-house	DPA	yes	yes
17	15		18/06/2003	2001 -	yes	yes	no	In-house	DPA	no	yes
18	16		5/09/2001	11/01/2000	yes	yes	DMA	In-house	DMAshp	no	no
19	17		27/02/2002	28/02/2002_	yes	yes/no	no	In-house	DPA	yes	yes
20	18		4/12/2002	1/01/2002	yes	no	TRUSTe	In-house	TRUSTe DPA	yes	yes
21	19		9/10/2003	31/12/2002	yes	no	no	in-house	DPA	yes	yes
22	20		20/05/2003	14/0/2003	yes	yes	TRUSTe	in-house	TRUSTe	no	no
23	21		6/12/2003	juin-02	yes	yes	no	in-house	DPA	no	yes
24	22		15/04/2002	6/08/2001	yes	yes/no	TRUSTe	TP	DPA & TRUSTe	yes	yes
25	23		3/07/2001	déc-89	yes	yes	CASRO	in-house	DPA	no	yes
26	24		27/05/2002	oct-98	yes	yes	no	in-house	DPA	no	yes
27	25		7/02/2002	2/7/2004	yes	yes	no	in-house	DPA	no	yes
28	26		8/03/2001	20/04/2001	yes	yes/no	no	in-house	DPA	yes	yes
29	27		17/09/2003	17/09/2003	yes	no	no	in-house	DPA	yes	yes
30	28		29/11/2003	15/06/2001	yes	no	no	in-house	DPA	yes	yes
31	29		28/1/2002	7/01/2001	yes	yes	DMAshp	in-house	DMAshp	no	no
32	30		25/06/2002	1/05/2002	yes	no	TRUSTe	TP	DPA & TRUSTe	yes	yes
33	31		24/02/2003	3/01/2003	yes	no	no	in-house	DPA	yes	yes
34	32		16/05/2003	9/01/2002	yes	yes	no	in-house	DPA	no	yes
35	33		28/05/2003	1/01/2000	yes	yes	no	in-house	AAA	no	no
36	34		22/03/2002	21/03/2002	yes	no	no	in-house	DPA	yes	yes
37	35		3/12/2003	13/02/2003	yes	yes	TRUSTe	TP	TRUSTe	no	no
38	36		25/6/2003	7/01/2003	yes	yes	no	in-house	DPA	no	yes
39	37		15/03/2001	31/01/2000	yes	yes/no	OPA	in-house	DPA	yes	yes
40	38		13/06/2002	5/01?	yes	yes	TRUSTe, CAUCE, DMAshp	in-house	DPA	no	yes
41	39		23/10/2001	20/01/2001	yes	yes/no	TRUSTe	in-house	DPA & TRUSTe	yes	yes
42	40		9/04/2001	sept-01	yes	yes	no	in-house	DMA	no	no
43	41		29/05/2001	26/01/2000	yes	yes	no	in-house	DPA	no	yes

Cellule: F2
Commentaire: FAQ 6 requires that the organization state the specific statutory body that has jurisdiction to hear claims against the organization.

Cellule: G2
Commentaire: FAQ 6 requires organizations to state the name of any privacy programs to which the organization belongs.

Cellule: I2
Commentaire: FAQ 6 requires organizationsto state the independent recourse mechanism that is available to investigate unresolved complaints.

Cellule: J2
Commentaire: FAQ 6 requires organizations processing human resources data to declare their commitment to cooperate with the DPA and to comply with the advice of such authortiy.

Cellule: F4
Commentaire: No, letter makes false assertion,

	A	B	C	D	E	F	G	H	I	J	K
1	**Table 2.1: SH Company Compliance with Notice Principle (as of November 3, 2003)**										
2	*Company*		*Clear*	*Conspicuous*	*Specified Purpose*	*Organization Contacts*	*Notice of secondary use*	*Third Party Disclosures*	*Notice of choice for use*	*Notice of Choice for dissemination*	*Statement of SH Compliance*
3	1		no	no	unclear	yes	no	yes	napp	no	no
4	2		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
5	3		no	no	unclear	yes	no	unclear	napp	unclear	yes
6	4		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
7	5		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
8	6		no	no	no	no	no	unclear	napp	unclear	no
9	7		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
10	8		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
11	9		no	no	yes	no	no	yes	napp	yes	no
12	10		yes	yes	yes	yes	yes	yes	yes	yes	yes
13	11		yes	yes	yes	yes	no	unclear	napp	unclear	yes
14	12		no	yes	unclear	yes	yes	yes	yes	no	yes
15	13		no	no	yes	yes	yes	no	no	napp	yes
16	14		no	no	unclear	yes	yes	yes	no	no	yes
17	15		yes	yes	yes	yes	no	no	napp	napp	yes
18	16		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
19	17		yes	yes	yes	no	yes	no	yes	napp	yes
20	18		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
21	19		yes	yes	yes	yes	yes	yes	yes	yes	yes
22	20		yes	yes	yes	yes	no	unclear	napp	unclear	yes
23	21		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
24	22		yes	no	yes	yes	no	yes	napp	unclear	yes
25	23		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
26	24		yes	yes	yes	no	unclear	unclear	unclear	no	yes
27	25		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
28	26		yes	yes	yes	yes	no	yes	napp	no	yes
29	27		no	yes	yes	yes	yes	yes	unclear	unclear	yes
30	28		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
31	29		unknown	unknown	unknown	unknown	unknown	unknown	unnown	unknown	unknown
32	30		yes	yes	yes	yes	no	yes	napp	yes	yes
33	31		yes	yes	yes	yes	yes	yes	yes	yes	yes
34	32		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
35	33		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
36	34		yes	yes	yes	yes	yes	yes	yes	yes	yes
37	35		yes	yes	unclear	yes	yes	yes	yes	yes	yes
38	36		yes	yes	yes	yes	yes	yes	yes	yes	yes
39	37		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
40	38		no	yes	no	yes	yes	unclear	yes	no	yes
41	39		no	yes	unclear	yes	no	unclear	napp	unclear	yes
42	40		no	no	unclear	yes	no	yes	napp	yes	yes
43	41		yes	yes	unclear	yes	no	yes	napp	yes	no
44											
45											
46											
47											
48											
49											
50											
51											
52											
53											

	A	B	C	D	E	F	G	H	I
1	**Table 2.2: Company Compliance with Choice Principle (as of November 3, 2003)**								
2	*Company*		*Opt-out (3rd party)*	*Opt-out (secondary use)*	*Clear*	*Conspicuous*	*Readily Available*	*Affordable*	*Opt-in (Sensitive Data)*
3	1		no	napp	napp	napp	napp	napp	napp
4	2		unknown	unknown	unknown	unknown	unknown	unknown	unknown
5	3		unclear	napp	yes	yes	yes	yes	napp
6	4		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
7	5		unknown	unknown	unknown	unknown	unknown	unknown	unknown
8	6		unclear	napp	no	no	no	no	napp
9	7		unknown	unknown	unknown	unknown	unknown	unknown	unknown
10	8		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
11	9		yes	napp	no	no	no	no	napp
12	10		yes	yes	yes	yes	no	no	napp
13	11		unclear	napp	no	yes	yes	no	napp
14	12		no	yes	no	yes	no	no	napp
15	13		napp	no	napp	napp	napp	napp	napp
16	14		no	no	napp	napp	napp	napp	napp
17	15		napp	napp	napp	napp	napp	napp	napp
18	16		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
19	17		napp	yes	no	no	no	no	yes
20	18		unknown	unknown	unknown	unknown	unknown	unknown	unknown
21	19		yes	yes	yes	yes	yes	unknown	unclear
22	20		unclear	napp	napp	napp	napp	napp	napp
23	21		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
24	22		unclear	napp	napp	napp	napp	napp	napp
25	23		unknown	unknown	unknown	unknown	unknown	unknown	unknown
26	24		no	unclear	no	no	no	no	no
27	25		unknown	unknown	unknown	unknown	unknown	unknown	unknown
28	26		no	napp	no	yes	napp	napp	napp
29	27		unclear	unclear	no	yes	no	no	unclear
30	28		unknown	unknown	unknown	unknown	unknown	unknown	unknown
31	29		unknown	unknown	unknown	unknown	unknown	unknown	unknown
32	30		yes	napp	yes	yes	no	no	yes
33	31		yes	yes	yes	yes	no	no	yes
34	32		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
35	33		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
36	34		yes	yes	yes	yes	no	no	yes
37	35		yes	yes	no	yes	yes	no	napp
38	36		yes	yes	yes	yes	no	no	yes
39	37		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
40	38		no	yes	napp	napp	npp	napp	napp
41	39		unclear	napp	no	yes	no	no	napp
42	40		yes	napp	yes	yes	no	no	napp
43	41		yes	napp	no	no	no	no	napp

Cellule: E2
Commentaire: The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."

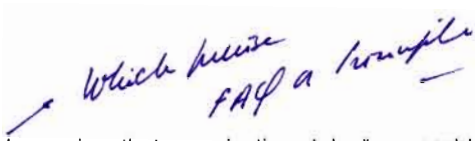
Cellule: F2
Commentaire: The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."

Cellule: G2
Commentaire: The SH Choice Principle requires that individuals "be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."
"Readily available" means that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out) and that the opt-out mechanism be transparent for data subjects.

Cellule: I21
Commentaire: "For sensitive Personal information, the company will give individuals the opportunity to affirmatively and explicitly (opt-in) consent to the disclosure of the information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual."

	A	B	C	D	E	F	G	H	I
1	**Table 2.3: Company Compliance with Onward Transfer Principle (as of November 3, 2003)**								
2	*Company*		*Notice of Onward Transfers*	*Choice*	*3rd Party Processor's Commitment to SH*				
3	1		yes	No	unclear				
4	2		unknown	unknown	unknown				
5	3		unclear	unclear	napp				
6	4		not applicable	Not applicable	not applicable				
7	5		unknown	unknown	unknown				
8	6		unclear	unclear	napp				
9	7		unknown	unknown	unknown				
10	8		not applicable	not applicable	not applicable				
11	9		yes	yes	napp				
12	10		yes	yes	napp				
13	11		unclear	unclear	napp				
14	12		yes	no	napp				
15	13		no	napp	yes				
16	14		yes	no	napp				
17	15		no	napp	napp				
18	16		not applicable	not applicable	not applicable				
19	17		no	napp	no				
20	18		unknown	unknown	unknown				
21	19		yes	yes	yes				
22	20		unclear	unclear	napp				
23	21		not applicable	not applicable	no				
24	22		yes	unclear	no				
25	23		unknown	unknown	unknown				
26	24		unclear	no	no				
27	25		unknown	unknown	unknown				
28	26		yes	no	no				
29	27		yes	unclear	unclear				
30	28		unknown	unknown	unknown				
31	29		unknown	unknown	unknown				
32	30		yes	yes	yes				
33	31		yes	yes	yes				
34	32		not applicable	not applicable	not applicable				
35	33		not applicable	not applicable	not applicable				
36	34		yes	yes	yes				
37	35		yes	yes	napp				
38	36		yes	yes	yes				
39	37		not applicable	not applicable	not applicable				
40	38		unclear	no	no				
41	39		unclear	unclear	no				
42	40		yes	yes	no				
43	41		yes	yes	no				

	A	B	C	D	E	F
1	**Table 2.4: Company Compliance with Security & Integrity Principles (as of November 3, 2003)**					
2	*Company*		*Reasonable Security Precautions*	*Relevance of Data for Specified Purpose*	*Compatible/ Authorized Processing for secondary use*	*Steps to Ensure Reliability for intended use*
3	1		no	unclear	napp	no
4	2		unknown	unknown	unknown	unknown
5	3		yes	unclear	napp	yes
6	4		unknown	not applicable	not applicable	not applicable
7	5		unknown	unknown	unknown	unknown
8	6		no	unclear	napp	no
9	7		unknown	unknown	unknown	unknown
10	8		no	not applicable	not applicable	not applicable
11	9		no	unclear	napp	no
12	10		yes	no	yes	no
13	11		yes	yes	napp	yes
14	12		yes	unclear	yes	yes
15	13		yes	unclear	no	no
16	14		no	unclear	no	no
17	15		no	unclear	napp	no
18	16		yes	not applicable	not applicable	not applicable
19	17		yes	unclear	yes	yes
20	18		unknown	unknown	unknown	unknown
21	19		yes	unclear	yes	yes
22	20		yes	unclear	napp	no
23	21		unknown	not applicable	not applicable	not applicable
24	22		yes	yes	napp	yes
25	23		unknown	unknown	unknown	unknown
26	24		yes	no	unclear	yes
27	25		unknown	unknown	unknown	unknown
28	26		yes	unclear	napp	no
29	27		unclear	unclear	unclear	unclear
30	28		unknown	unknown	unknown	unknown
31	29		unknown	unknown	unknown	unknown
32	30		yes	yes	napp	yes
33	31		yes	yes	yes	yes
34	32		unknown	not applicable	not applicable	not applicable
35	33		yes	not applicable	not applicable	not applicable
36	34		yes	yes	yes	yes
37	35		yes	unclear	yes	no
38	36		yes	unclear	yes	yes
39	37		unclear	not applicable	not applicable	not applicable
40	38		yes	unclear	yes	no
41	39		yes	unclear	napp	no
42	40		no	unclear	napp	no
43	41		unclear	unclear	napp	no



Cellule: C2
Commentaire: SH Security Principle requires that organizations take "reasonable precautions to protect [data] from loss, misuse and unauthorized access, disclosure, alteration and destruction. " Any site stating that it uses encryption to transmit data will qualify under this SH principle.

Cellule: D2
Commentaire: SH Data Integrity Principle requires that "personal information must be relevant for the purposes for which it is to be used." The policy must indicate in some way that the data is relevant for the specified purpose.

Cellule: E2
Commentaire: SH Data Integrity Principle provides "An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual."

Cellule: F2
Commentaire: SH Data Integrity Principle requires that "an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current."

Cellule: F22
Commentaire: no representation made

Cellule: C39
Commentaire: security entry is drafted as an exonoration clause in case X's clients would violate security

Cellule: C43
Commentaire: only representation about password protection

	A	B	C	D	E	F
1	**Table 2.5: Company Compliance with Access Principle (as of November 3, 2003)**					
2	*Company*		*Reasonable Access Provided*	*Reasonable Cost for Access*	*Correction / Amendment of inaccurate data*	*Deletion of inaccurate data*
3	1		no	napp	no	no
4	2		unknown	unknown	unknown	unknown
5	3		no	napp	no	no
6	4		not applicable	not applicable	not applicable	not applicable
7	5		unknown	unknown	unknown	unknown
8	6		no	not app	no	no
9	7		unknown	unknown	unknown	unknown
10	8		not applicable	not applicable	not applicable	not applicable
11	9		no	napp	no	no
12	10		no	no	yes	no
13	11		no	no	yes	no
14	12		no	no	yes	yes
15	13		no	napp	yes	no
16	14		no	napp	no	no
17	15		no	napp	no	no
18	16		not applicable	not applicable	not applicable	not applicable
19	17		yes	no	yes	yes
20	18		unknown	unknown	unknown	unknown
21	19		unclear	no	yes	yes
22	20		no	napp	yes	no
23	21		not applicable	not applicable	not applicable	not applicable
24	22		no	napp	no	no
25	23		unknown	unknown	unknown	unknown
26	24		yes	no	unclear	unclear
27	25		unknown	unknown	unknown	unknown
28	26		no	napp	yes	yes
29	27		yes	no	yes	yes
30	28		unknown	unknown	unknown	unknown
31	29		unknown	unknown	unknown	unknown
32	30		yes	no	yes	no
33	31		yes	no	yes	yes
34	32		not applicable	not applicable	not applicable	not applicable
35	33		not applicable	not applicable	not applicable	not applicable
36	34		yes	no	yes	yes
37	35		yes	no	yes	no
38	36		yes	no	yes	yes
39	37		not applicable	not applicable	not applicable	not applicable
40	38		no	napp	yes	no
41	39		no	napp	yes	no
42	40		no	napp	no	no
43	41		no	no	unclear	unclear

Cellule: C12
Commentaire: The access is conditioned to specific situations

Cellule: F13
Commentaire: " changing and modifying information previously provided",

Cellule: C43
Commentaire: access to "my account". Quid about access to user profiles, etc.

	A	B	C	D	E	F	G
1	**Table 3.1: Company Satisfaction of SH Enforcement Principles (as of November 3, 2003)**						
2	*Company*		*Independent Recourse Mechanisms pursuant to FAQ 5*	*Independent Recourse Mechanisms pursuant to FAQ 11*	*Verification of Policy Statements/ Implementation*	*Obligation to remedy problem*	*Sanctions for Violations*
3	1		yes	DPA	8/12/2004	no	no
4	2		yes	DPA	25/02/2004	unknown	unknown
5	3		no	AAA	19/08/2004	unclear	no
6	4		no	DMAshp	27/11/2003	not applicable	not applicable
7	5		yes	DPA	24/05/2004	unknown	unknown
8	6		yes	DPA	6/03/2004	no	no
9	7		yes	BBB & DPA	27/01/2004	no	no
10	8		no	BBB	9/04/2004	not applicable	not applicable
11	9		yes	DPA	20/09/2004	no	no
12	10		no	TRUSTe & BBB	7/01/2004	unclear	yes
13	11		yes	DPA	3/07/2004	yes	yes
14	12		yes	DPA & TRUSTe	15/01/2004	no	yes
15	13		yes	DPA & AAA	6/03/2003	no	no
16	14		yes	DPA	15/11/2003	no	no
17	15		yes	DPA	18/06/2003	no	no
18	16		no	DMAshp	5/09/2004	not applicable	not applicable
19	17		yes	DPA	27/02/2004	yes	yes
20	18		yes	TRUSTe DPA	4/12/2003	no	yes
21	19		yes	DPA	9/10/2004	no	no
22	20		no	TRUSTe	20/05/2004	no	yes
23	21		yes	DPA	6/12/2003	not applicable	not applicable
24	22		yes	DPA & TRUSTe	15/04/2002	no	yes
25	23		yes	DPA	3/07/2003	unknown	Unknown
26	24		yes	DPA	27/05/2004	no	no
27	25		yes	DPA	7/02/2004	unknown	unknown
28	26		yes	DPA	8/03/2003	no	no
29	27		yes	DPA	17/9/2004	no	no
30	28		yes	DPA	7/12/2004	unknown	unknown
31	29		no	DMAshp	28/01/2004	unclear	yes
32	30		yes	DPA & TRUSTe	25/06/2004	no	yes
33	31		yes	DPA	24/02/2004	no	no
34	32		yes	DPA	16/05/2004	not applicable	not applicable
35	33		no	AAA	2805/2004	not applicable	not applicable
36	34		yes	DPA	22/03/2004	yes	yes
37	35		no	TRUSTe	3/12/2004	no	yes
38	36		yes	DPA	7/01/2003	no	no
39	37		yes	DPA	15/03/2004	not applicable	not applicable
40	38		yes	DPA	13/06/2004	no	no
41	39		yes	DPA & TRUSTe	23/10/2004	no	yes
42	40		no	DMA	4/09/2004	no	no
43	41		yes	DPA	29/05/2001	no	yes

Cellule: D2
Commentaire: SH Enforcement Principle requires "readily available and affordable independent recourse mechanisms." This element of the SH may be satisfied pursuant to FAQ5 or FAQ 11.

Cellule: E2
Commentaire: SH Enforcement Principles requires that organizations verify the statements made in their policy certifications and the implementation of their policies at least once a year. This column shows the deadline for the first verification.

Cellule: F2
Commentaire: SH Enforcement Principle states that enforcement must include "obligations to remedy problems arising out of failure to comply with the Principles."

Cellule: G2
Commentaire: SH Enforcement Principle requires that "sanctions must be sufficiently rigorous to ensure compliance by organizations." Any company that has elected DPA as a recourse mechanism, but that does not fully satisfy FAQ 5, cannot satisfy the sanctions requirement.

Cellule: G9
Commentaire: Even if BBB foresees sanctions, the company only adheres to BBB for the data it receives as processor, then, where there's no a real obligation of enforcement. However, in the privacy policy dealing with HR data nothing is represented in this regard.

	A	B	C	D	E
1	**Table 3.2: Company Conformity to FAQ 5 (as of November 3, 2003)**				
2	*Company*		*Elects DPA enforcement*	*Co-operates with DPAs*	*Agrees to comply with DPA advice*
3	1		yes	Certif	no
4	2		yes	Certif	unknown
5	3		no	no	napp
6	4		no	no	napp
7	5		yes	Certif	unknown
8	6		yes	Both	no
9	7		yes	Both	unknown
10	8		no	no	napp
11	9		yes	Certif	no
12	10		no	no	napp
13	11		yes	Both	no
14	12		yes	Certif	no
15	13		yes	Certif	no
16	14		yes	Certif	no
17	15		yes	Certif	no
18	16		no	no	napp
19	17		yes	Both	yes
20	18		yes	Certif	unknown
21	19		yes	Both	no
22	20		no	no	napp
23	21		yes	Certif	napp
24	22		yes	Certif	no
25	23		yes	Certif	no
26	24		yes	Certif	no
27	25		yes	Certif	unknown
28	26		yes	Certif	no
29	27		yes	Both	no
30	28		yes	Certif	unknown
31	29		no	no	napp
32	30		yes	Certif	no
33	31		yes	Certif	no
34	32		yes	Certif	unknown
35	33		no	no	napp
36	34		yes	Both	yes
37	35		no	no	napp
38	36		yes	Certif	no
39	37		yes	Certif	no
40	38		yes	Certif	no
41	39		yes	Certif	no
42	40		no	no	napp
43	41		yes	Certif	no

Cellule: C2
Commentaire: This is also listed in FAQ 11.

	A	B	C	D	E	F	G	H	I	J	K
1	Table 3.3: Company Conformity to FAQ 11 (as of November 3, 2003)										
2	*Company*		*US Legal or Regulatory Supervision*	*Independence of recourse mechanism*	*Readily available/affordable recourse*	*Transparency of dispute resolution procedures*	*Company agrees to reverse effects of breach*	*SH Compliant Future Processing*	*Cessation of processing of data for harmed individual*	*Publicity for Findings*	*Sanctions*
3	1		no	yes	yes	no	no	no	no	no	no
4	2		no	yes	yes	unknown	unknown	unknown	unknown	unknown	unknown
5	3		no	yes	yes	yes	unclear	no	unclear	no	no
6	4		no	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
7	5		no	yes	yes	unknown	unknown	unknown	unknown	unknown	unknown
8	6		no	yes	yes	yes	no	no	no	no	no
9	7		no	yes	yes	no	no	no	no	no	no
10	8		no	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
11	9		no	yes	yes	yes	no	no	no	no	no
12	10		no	yes	yes	yes	unclear	no	no	unclear	yes
13	11		no	yes	yes	yes	yes	yes	no	no	yes
14	12		no	yes	yes	no	unclear	no	no	unclear	yes
15	13		no	yes	yes	no	unclear	no	unclear	no	no
16	14		no	yes	yes	no	no	no	no	no	no
17	15		no	yes	yes	no	no	no	no	no	no
18	16		no	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
19	17		no	yes	yes	yes	yes	yes	yes	yes	yes
20	18		no	yes	yes	unknown	no	no	no	no	yes
21	19		no	yes	yes	yes	no	no	no	no	no
22	20		no	yes	yes	yes	no	no	no	no	yes
23	21		no	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
24	22		no	yes	yes	yes	no	no	no	no	yes
25	23		no	yes	yes	unknown	unknown	unknown	unknown	unknown	unknown
26	24		no	yes	yes	no	no	no	no	no	no
27	25		no	yes	yes	unknown	unknown	unknown	unknown	unknown	unknown
28	26		no	yes	yes	no	no	no	no	no	no
29	27		no	yes	yes	yes	no	no	no	no	no
30	28		no	yes	yes	unknown	unknown	unknown	unknown	unknown	unknown
31	29		no	yes	yes	no	unclear	yes	unclear	yes	yes
32	30		no	yes	yes	yes	no	no	no	no	yes
33	31		no	yes	yes	no	no	no	no	no	no
34	32		no	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
35	33		no	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
36	34		no	yes	yes	yes	yes	yes	yes	yes	yes
37	35		no	yes	yes	yes	no	no	no	no	yes
38	36		no	yes	yes	no	no	no	no	no	no
39	37		no	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
40	38		no	yes	yes	no	no	no	no	no	no
41	39		no	yes	yes	yes	no	no	no	no	yes
42	40		no	yes	yes	no	no	no	no	no	no
43	41		no	yes	yes	no	no	no	no	no	yes

Cellule: C2
Commentaire: FAQ 11 allows the Enforcement Principle to be satisfied by "compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution."

Cellule: D2
Commentaire: FAQ 11 states that "Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record." Under FAQ 11, a company may satisfy this requirement by making a commitment to cooperate with the DPA.

Cellule: F2
Commentaire: FAQ 11 requires that "recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works." If a company has elected DPA dispute settlement and indicates such mechanism in its privacy policy, then the process will be considered transparent.

Cellule: G2
Commentaire: FAQ 11 requires that the remedies available in the dispute resolution process include the reversal of the effects of non-compliance.

Cellule: H2
Commentaire: FAQ 11 requires that the dispute resolution proceeding remedy result in future processing that will be in conformity with the SH Principles.

Cellule: I2
Commentaire: FAQ 11 requires that the dispute resolution proceeding remedy result in the cessation, when appropriate, of or processing the personal data of the individual who brought the complaint.

Cellule: J2
Commentaire: FAQ 11 states that "Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances."

Cellule: K2
Commentaire: FAQ 11 requires sanctions which "could include suspension and removal of a seal, compensation for individuals for losses ... and injuncive orders." In addition, FAQ 11 requires that sanctions include "the requirement to delete data in certain circumstances" depending on the dispute resolution body's interpretation of the data's sensitivity. Any company that has elected enforcement by a DPA, but has not agreed to abide by the DPA decision does not qualify for sanctions.

Cellule: J12
Commentaire: This company has choosen two ADRs, one provides for publication, the other one not.

	A	B	C	D	E	F	G	H
1	**Table A: Incorporation of SH Notice Principles in Privacy Program Rules**							
2	*Self-Regulatory Privacy Program*		*Program Contacts*	*Statement of SH Compliance*	*Clear/ Conspicuous Member Policy*	*Members Specify Purposes*	*Members Disclose 3rd Party Recipients*	*Data Subject Choice for use/ dissemination*
3	1		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
4	2		Yes	No	Yes	Yes	Yes	No
5	3		yes	no	No	Yes	No	napp
6	4		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
7	5		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
8	6		no	no	yes	unclear	yes	yes
9	7		Yes	No	Yes	Yes	Yes	Yes
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								
39								
40								
41								
42								
43								
44								
45								
46								
47								
48								
49								
50								
51								
52								
53								
54								
55								
56								
57								
58								

Cellule: H4
Commentaire: The "Privacy Program Eligibilty Requirements" only include data subject choice for direct marketing uses of personal information.

	A	B	C	D	E	F	G	H
1	**Table B: Incorporation of SH Choice Principle in Privacy Program Rules**							
2	*Self-Regulatory Privacy Program*		*Opt-out (3rd party)*	*Opt-out (secondary use)*	*Clear/ Conspicuous*	*Readily Available*	*Affordable*	*Opt-in (Sensitive Data)*
3	1		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
4	2		No	No	Yes	No	No	No
5	3		napp	No	No	No	No	No
6	4		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
7	5		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
8	6		yes	yes	yes	no	no	no
9	7		Yes	Yes	No	No	No	No
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								

Cellule: F2
Commentaire: "Readily available" means that a medium comparable to that of the original data collection must be available to opt-out (e.g. online data collection should use online opt-out.)

Cellule: C4
Commentaire: The Privacy Program Eligibility Requirements provide an opt-out only to those "outside parties or corporate affiliates operating under a different privacy notice." However, the Privacy Program Assessment Questionnaire states that transfers to outside parties for direct marketing "must provide individuals with the ability to prevent these transfers." Transfers for other uses are not covered by the required opt-out.

Cellule: D4
Commentaire: The Privacy Program Eligibility Requirements only mandate an opt-out for direct marketing uses.

Cellule: D5
Commentaire: The opt-out is available for unsolicited email messages. The statement mentions no other opt-out.

Cellule: E9
Commentaire: The program rules do not explicitly indicate that choice must be offered in a clear and conspicuous manner.

Cellule: F9
Commentaire: The program rules do not impose any requirements on the means to exercise choice.

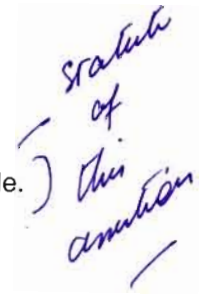
	A	B	C	D	E
1	**Table C: Incorporation of Onward Transfer Principle in Privacy Program Rules**				
2	*Self-Regulatory Privacy Program*		*Notice of Onward Transfers*	*Choice*	*3rd Party Processor's Commitment to SH*
3	1		not applicable	not applicable	not applicable
4	2		no	no	no
5	3		no	no	no
6	4		not applicable	not applicable	not applicable
7	5		not applicable	not applicable	not applicable
8	6		yes	yes	no
9	7		yes	yes	no
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					

	A	B	C	D	E	F
1	**Table D: Incorporation of Security & Integrity Principles in Privacy Program Rules**					
2	*Self-Regulatory Privacy Program*		*Reasonable Security Precautions*	*Relevance of Data*	*Compatible/ Authorized Processing for Secondary Use*	*Steps to Ensure Reliability for Intended Use*
3	1		not applicable	not applicable	not applicable	not applicable
4	2		Yes	No	No	No
5	3		No	No	Yes	Yes
6	4		not applicable	not applicable	not applicable	not applicable
7	5		not applicable	not applicable	not applicable	not applicable
8	6		yes	no	yes	yes
9	7		Yes	No	Yes	Yes
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						

Cellule: C2

Commentaire:

Any site stating that it uses encryption to transmit data will qualify under this SH Principle.



	A	B	C	D	E	F	G
1	**Table E: Incorporation of SH Access Principle in Privacy Program Rules**						
2	*Self-Regulatory Privacy Program*		*Reasonable Access Provided*	*Reasonable Cost for Access*	*Correction of inaccurate data*	*Amendment of inaccurate data*	*Deletion of inaccurate data*
3	1		not applicable	not applicable	not applicable	not applicable	not applicable
4	2		yes	yes	yes	no	no
5	3		no	napp	no	no	no
6	4		not applicable	not applicable	not applicable	not applicable	not applicable
7	5		not applicable	not applicable	not applicable	not applicable	not applicable
8	6		yes	no	yes	yes	no
9	7		Yes	No	Yes	Yes	Yes
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							

Cellule: C9
Commentaire: The program rules contain an access principle that applies only to members who agree to an additional EU policy.

Cellule: E9
Commentaire: This applies only to members who have signed the additional EU addendum.

Cellule: F9
Commentaire: This applies only to members who have signed the additional EU addendum.

Cellule: G9
Commentaire: This applies only to members who have signed the additional EU addendum.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Table F: Incorporation of Enforcement Principles in Dispute Resolution (SH & FAQ 11)												
2	*Self-Regulatory Privacy Program*		*Independent Dispute Resolution Body ("DRB")*	*Investigation of each complaint*	*Readily available/ Affordable Recourse*	*Transparency of Recourse Procedures*	*DRB Obtains Reversal of Effects of Breach*	*DRB Obtains SH Compliant Future Processing*	*DRB Obtains Cessation of Processing*	*Compensation for Harm*	*Privacy Program Sanctions*	*Publication of DRB Sanctions*	*Mandatory Referral of DRB Sanctions*
3	1		yes	yes	yes	yes	unclear	no	unclear	unclear	napp	no	no
4	2		unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
5	3		yes	yes	yes	yes	unclear	unclear	no	no	unclear	no	no
6	4		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
7	5		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
8	6		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
9	7		yes	yes	yes	yes	unclear	yes	unclear	yes	yes	yes	unclear
10	8		no	unclear	no	no	no	yes	yes	yes	yes	no	no
11	9		yes	yes	yes	no	unclear	unclear	unclear	unclear	N/A	no	no
12	10		not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable	not applicable
13	11		yes	yes	yes	yes	no	no	no	no	yes	no	no
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													
26													
27													
28													
29													
30													
31													
32													
33													
34													
35													
36													
37													
38													
39													
40													
41													
42													
43													
44													
45													
46													
47													
48													
49													
50													
51													
52													
53													
54													
55													
56													
57													
58													

Cellule: I2
Commentaire: FAQ 11 requires that the DRB be able to obtain the cessation of processing of data for the harmed individual.

Cellule: K2
Commentaire: FAQ 11. (e.g. suspension or removal of seal)

Cellule: G3
Commentaire: *The arbitrator should be empowered to grant whatever relief would be available in court under law or in equity.

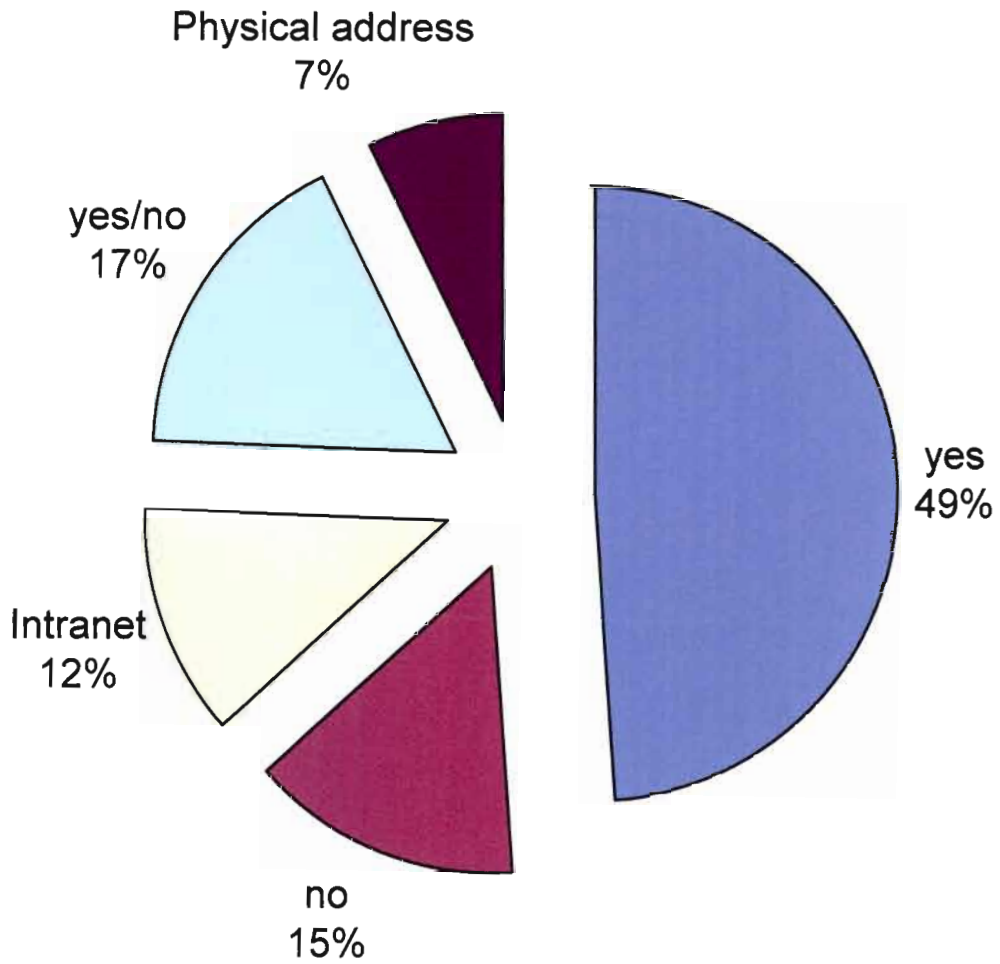
Cellule: F9
Commentaire: The recourse procedures are hard to find on the web site and are incomplete.

Cellule: C10
Commentaire: There's no representation concerning the independence of the body, nor a description of the composition of it.

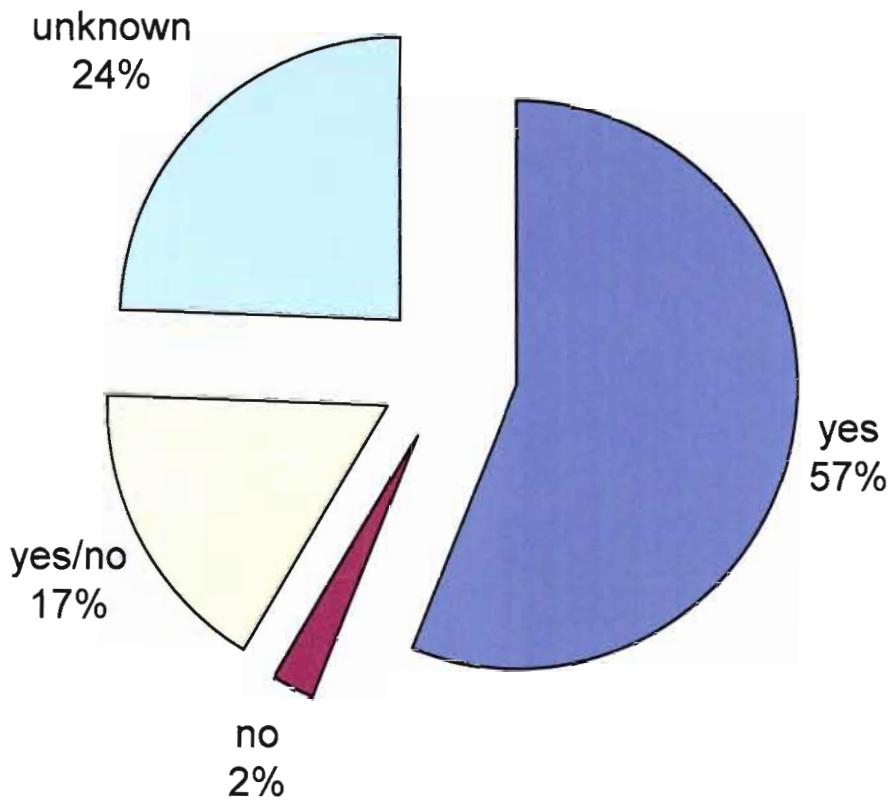
Cellule: D11
Commentaire: The arbitration provision must allow for the discovery or exchange of non-privileged information relevant to the dispute

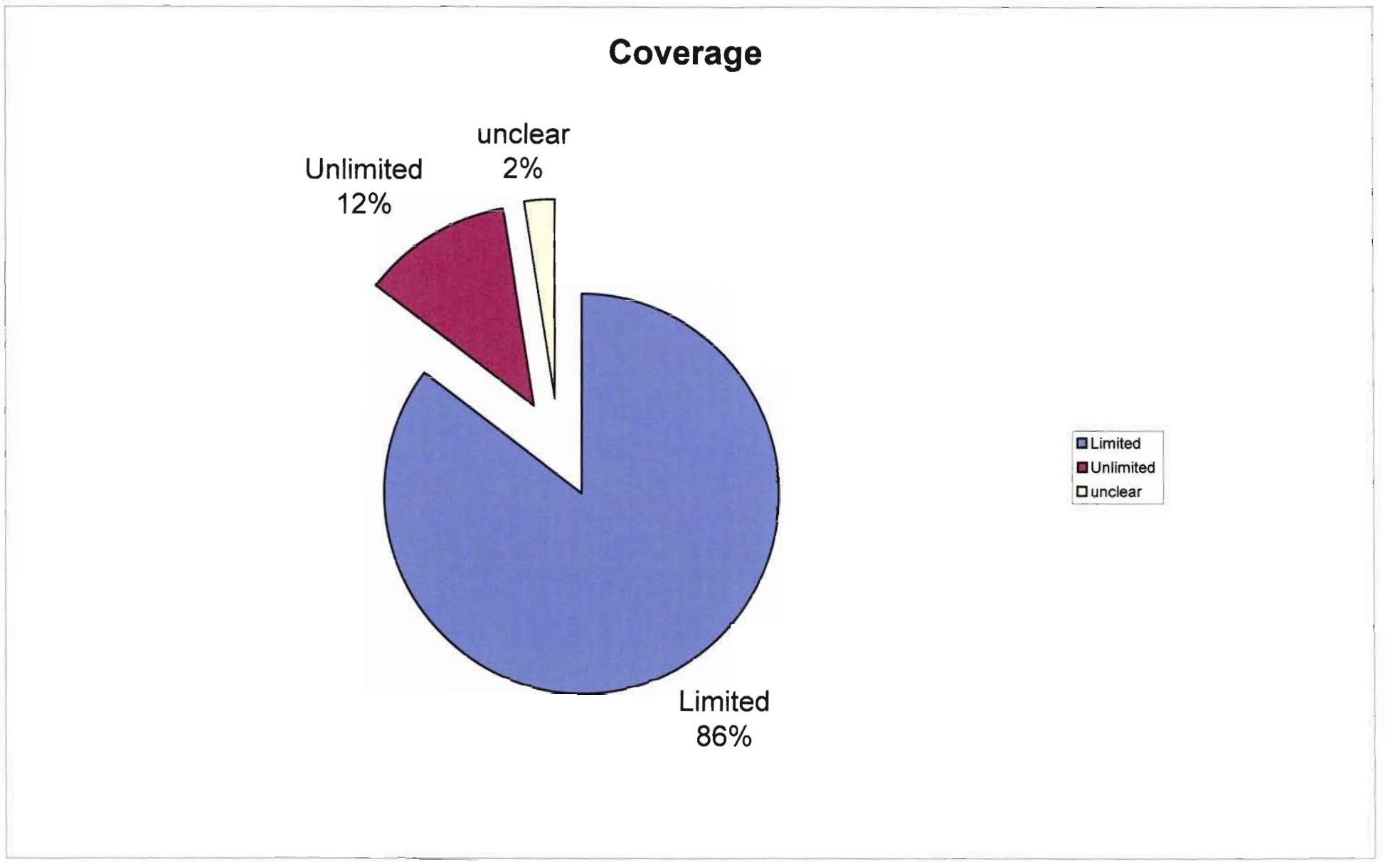
Table 1.1

Public Disclosure of Privacy Policy

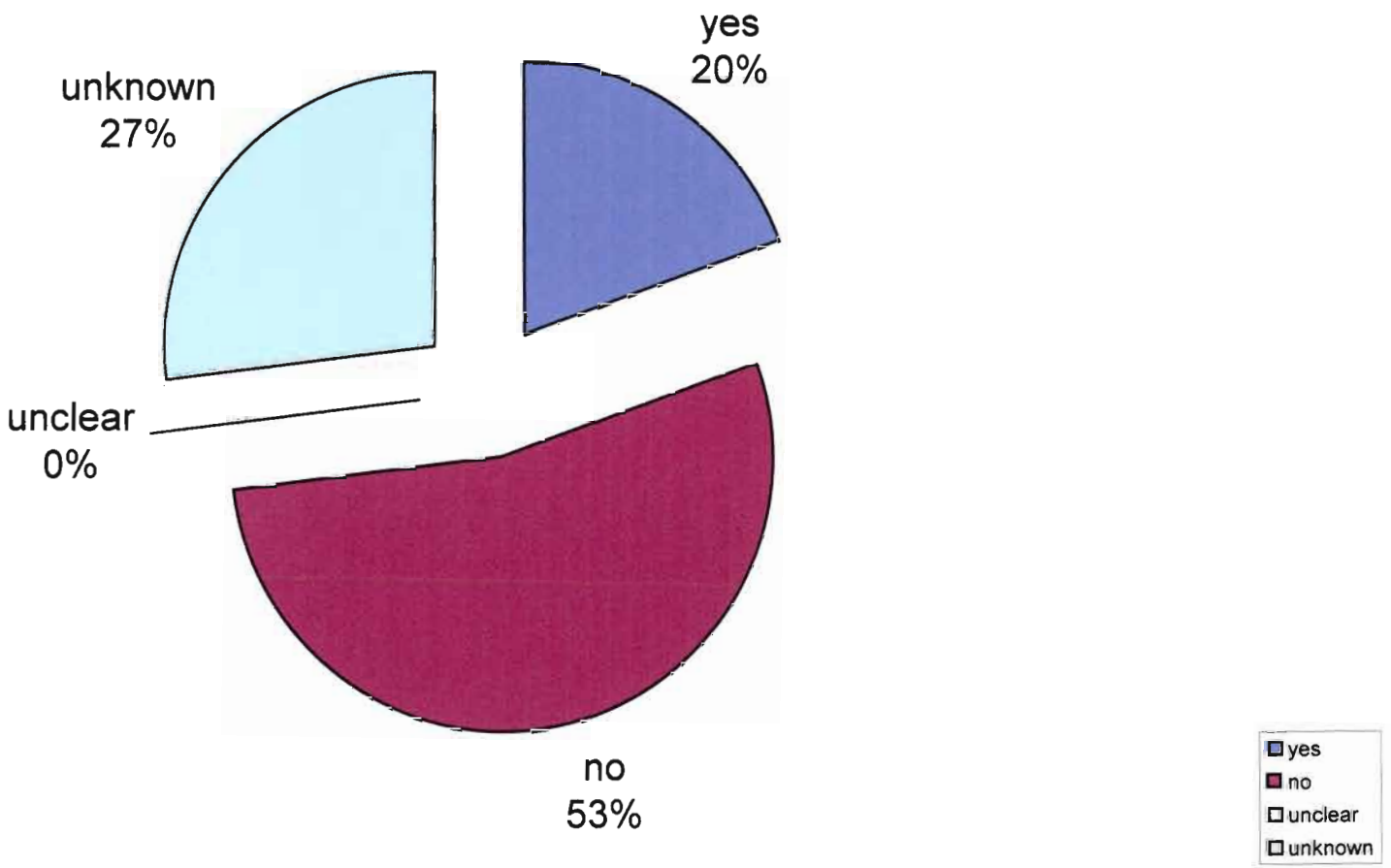


Printable Policy

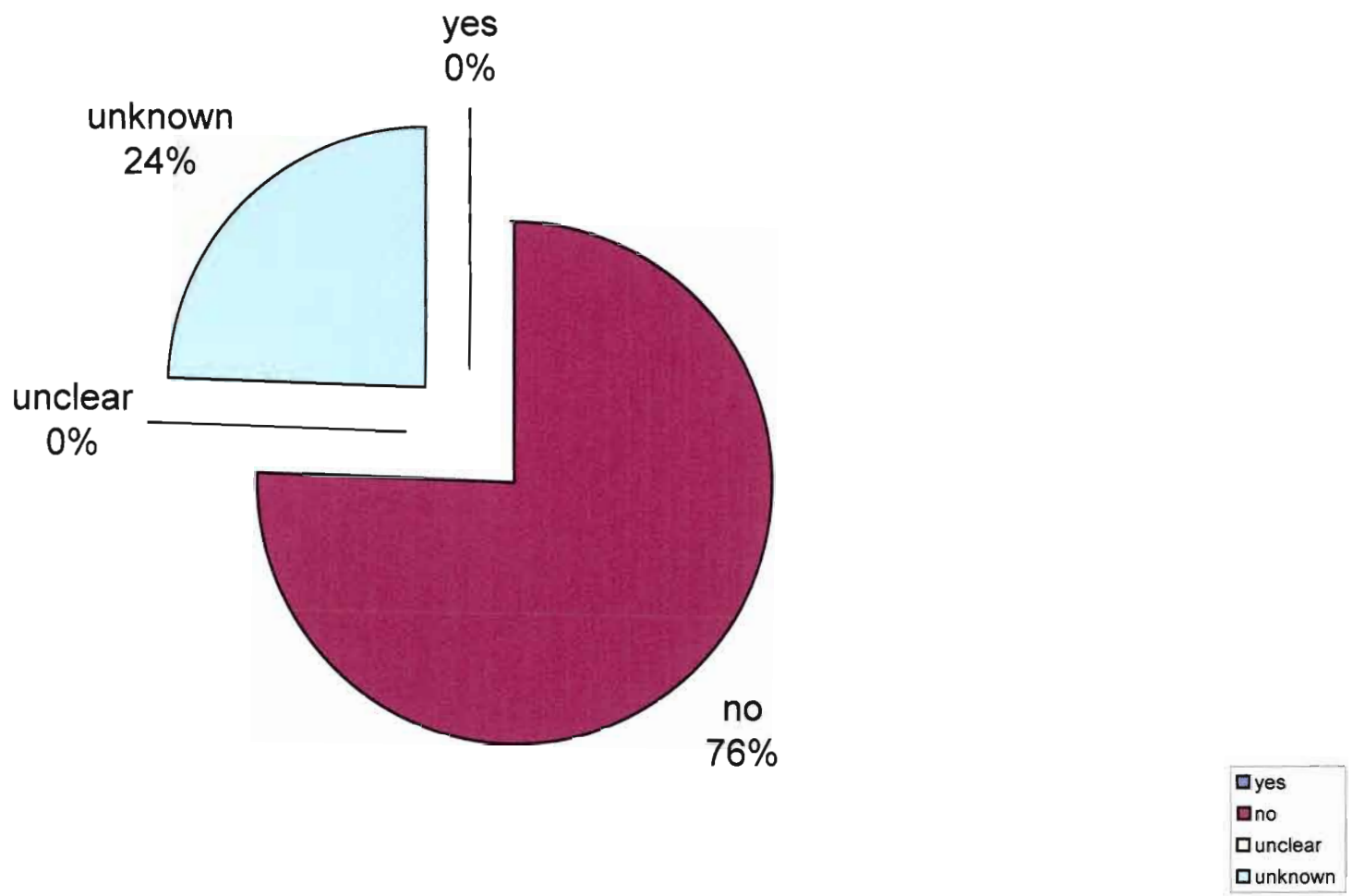



Coverage
unclear
2%
Unlimited
12%
Limited
86%
Limited
Unlimited
unclear

Policy Applies to EU Data Indefinitely



Policy Signals US Law Preventing Compliance



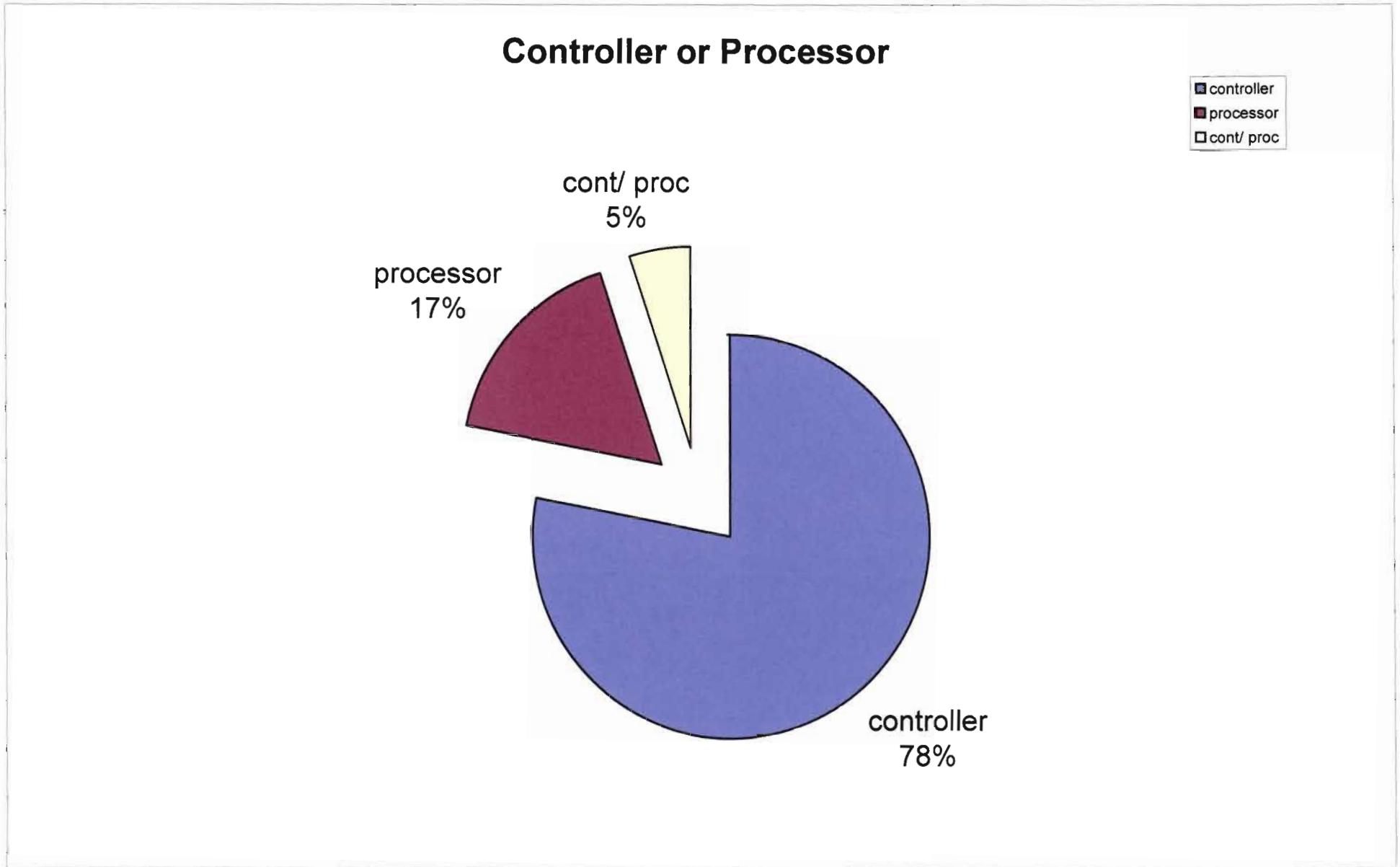
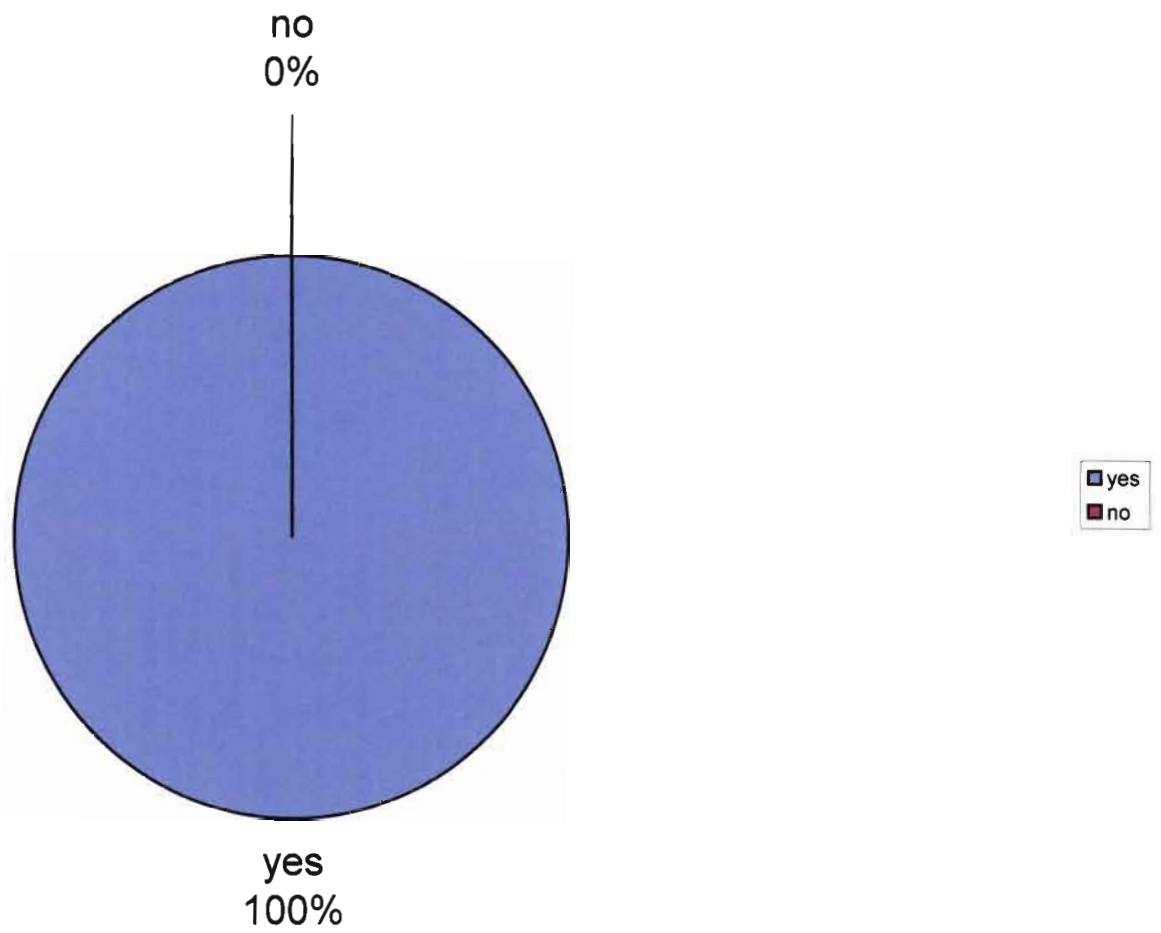
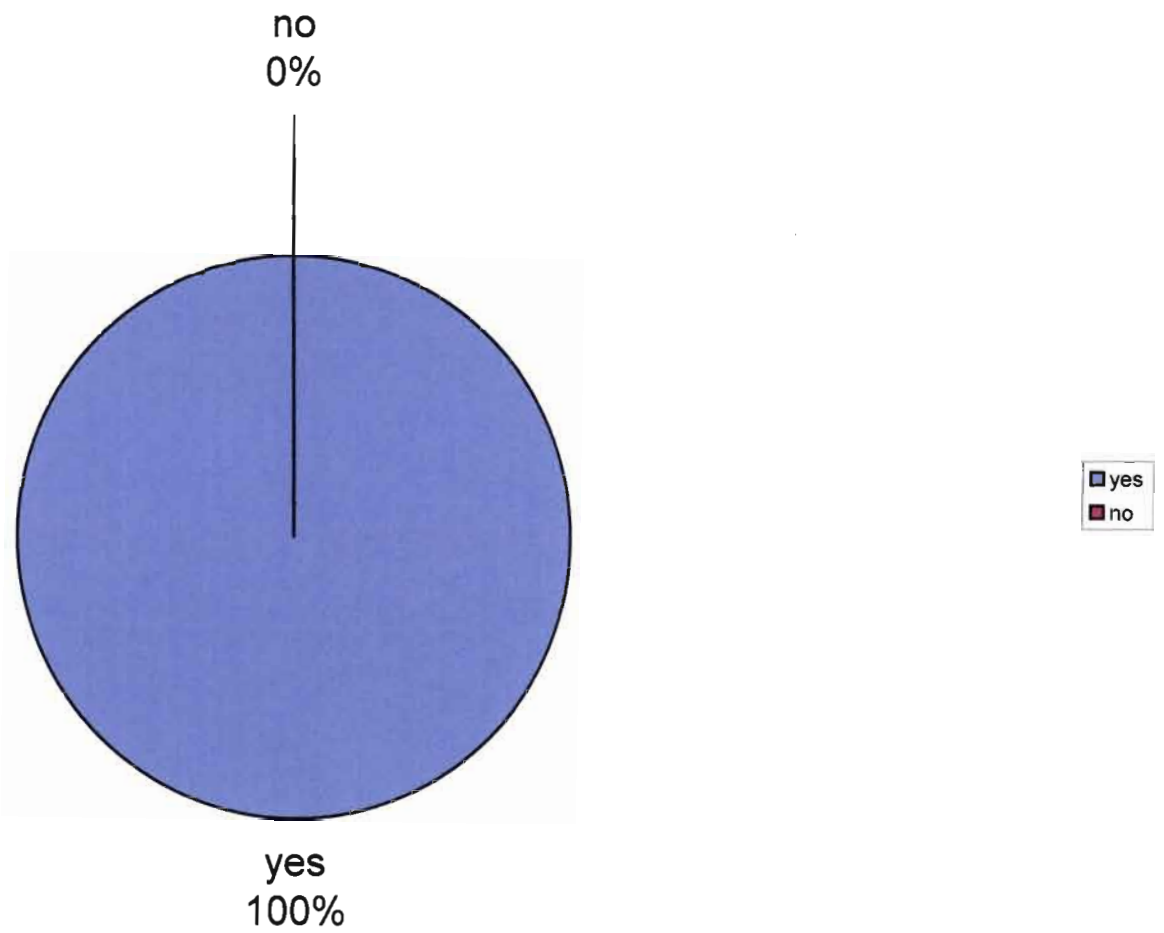

Controller or Processor
controller
processor
cont/ proc
cont/ proc
5%
processor
17%
controller
78%

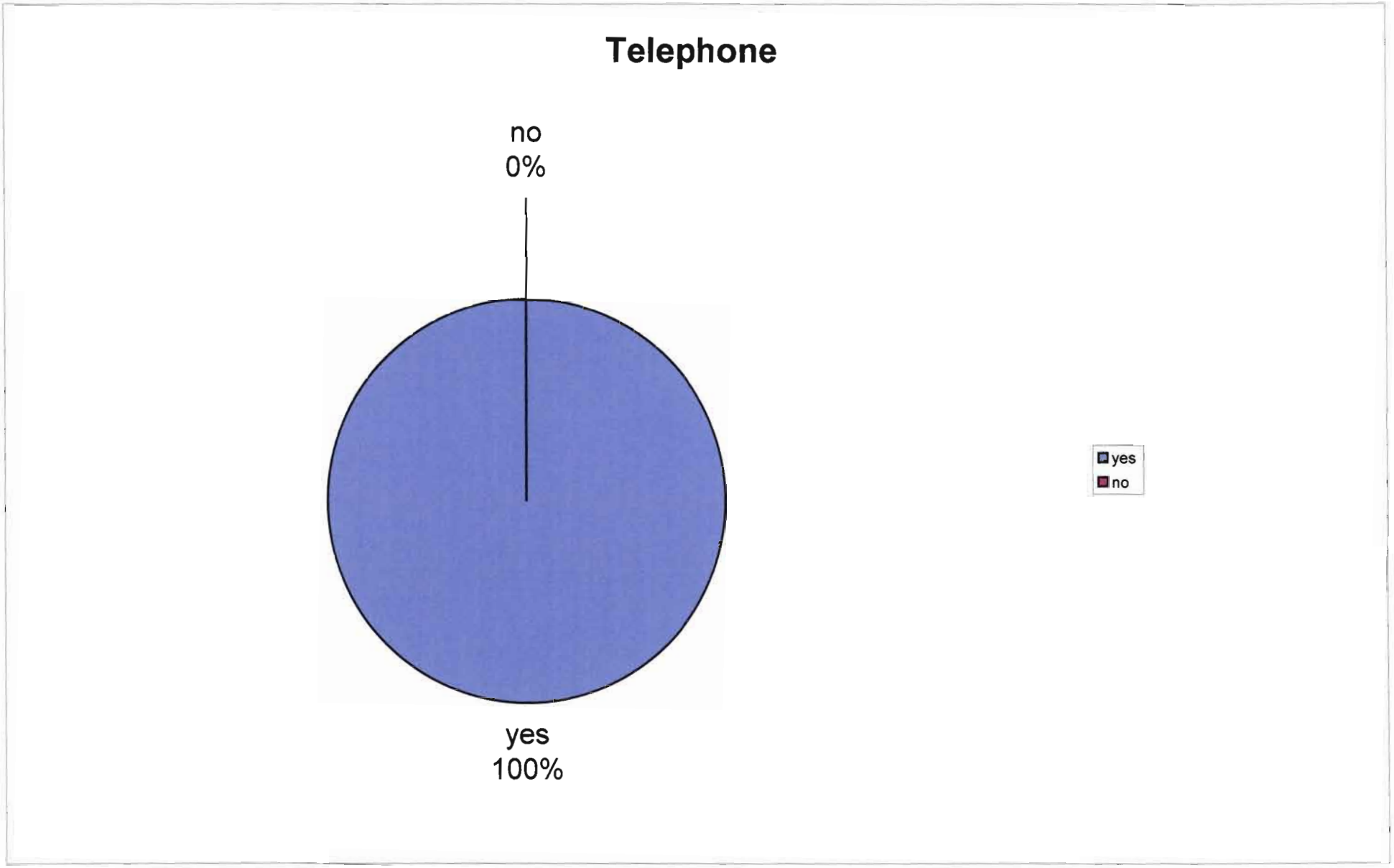
Table 1.2

Name Reported

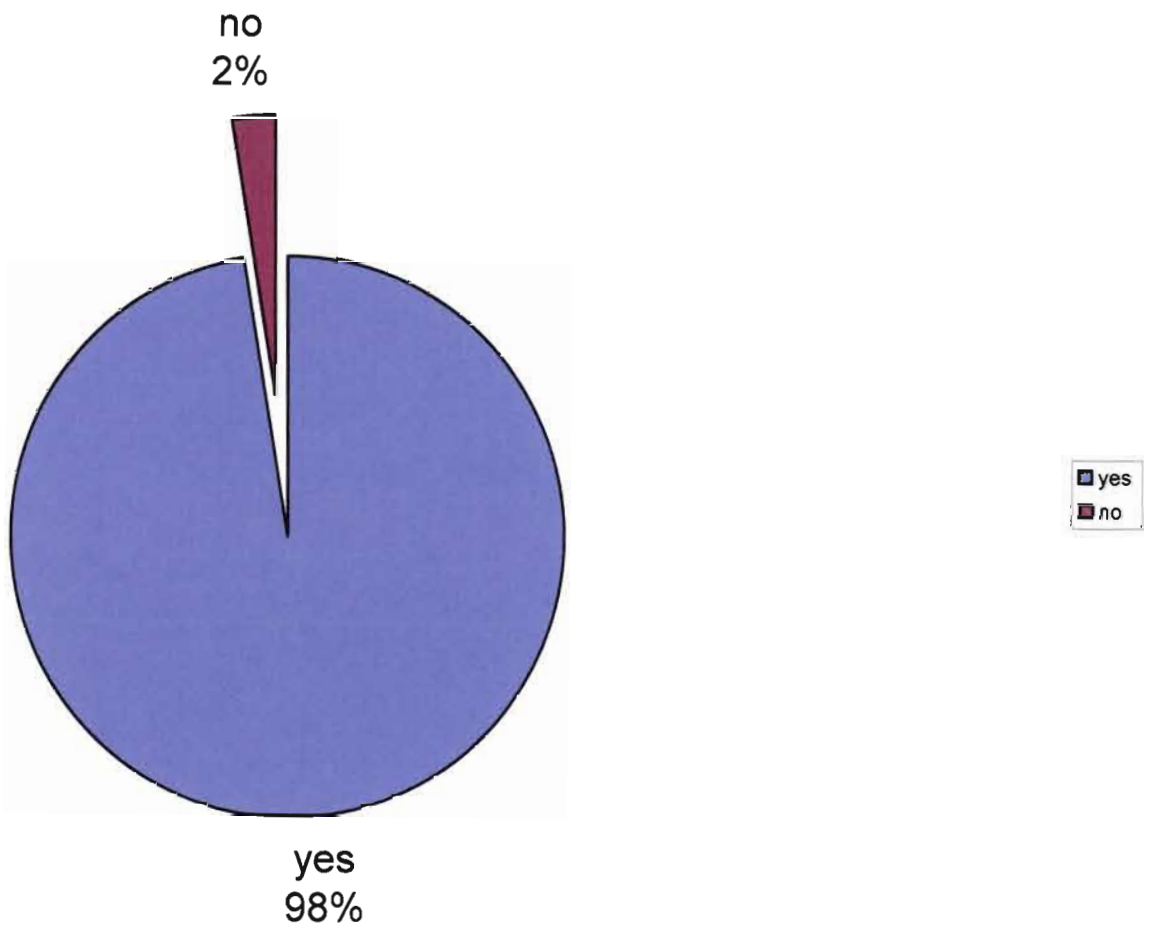


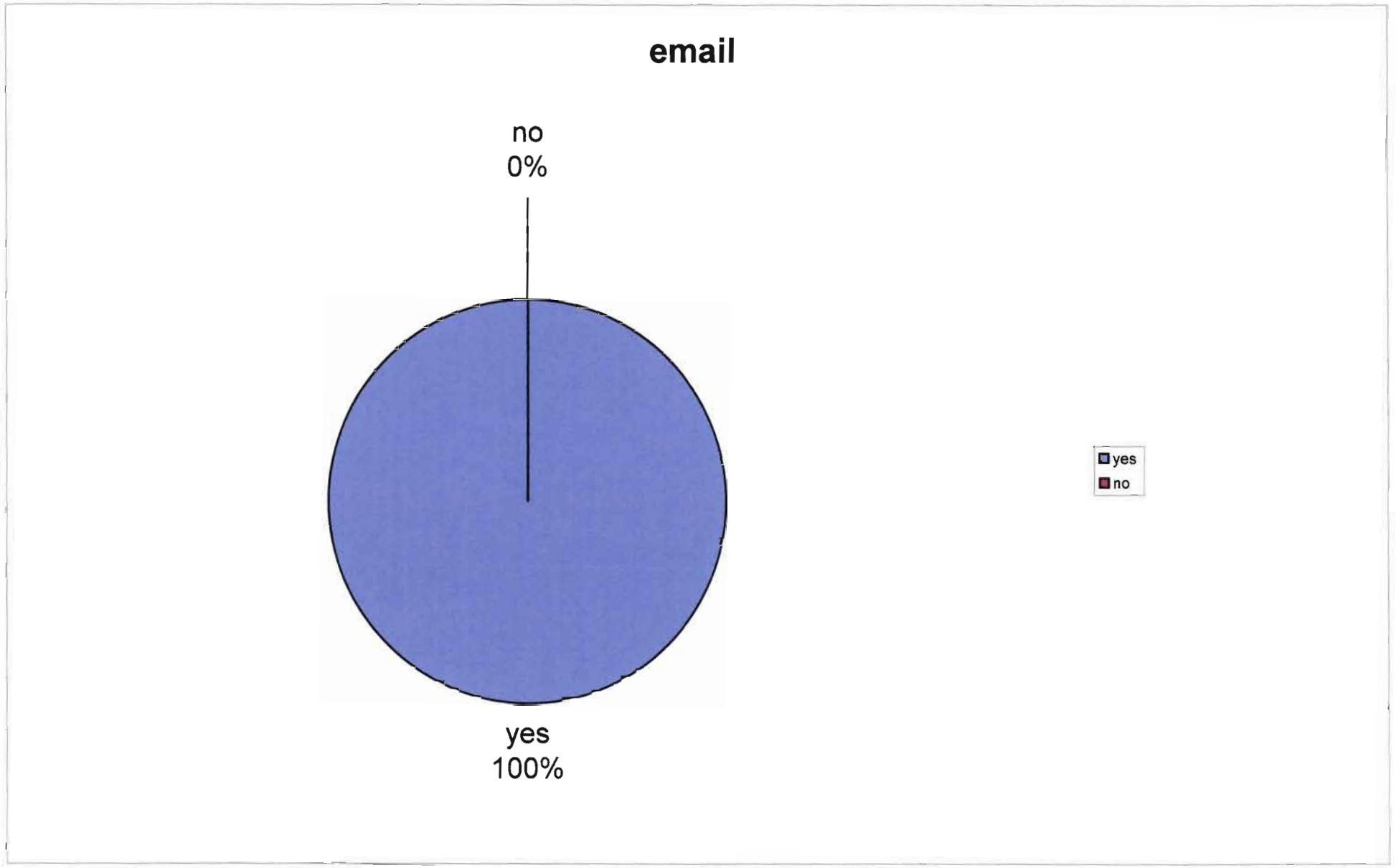
Address Reported



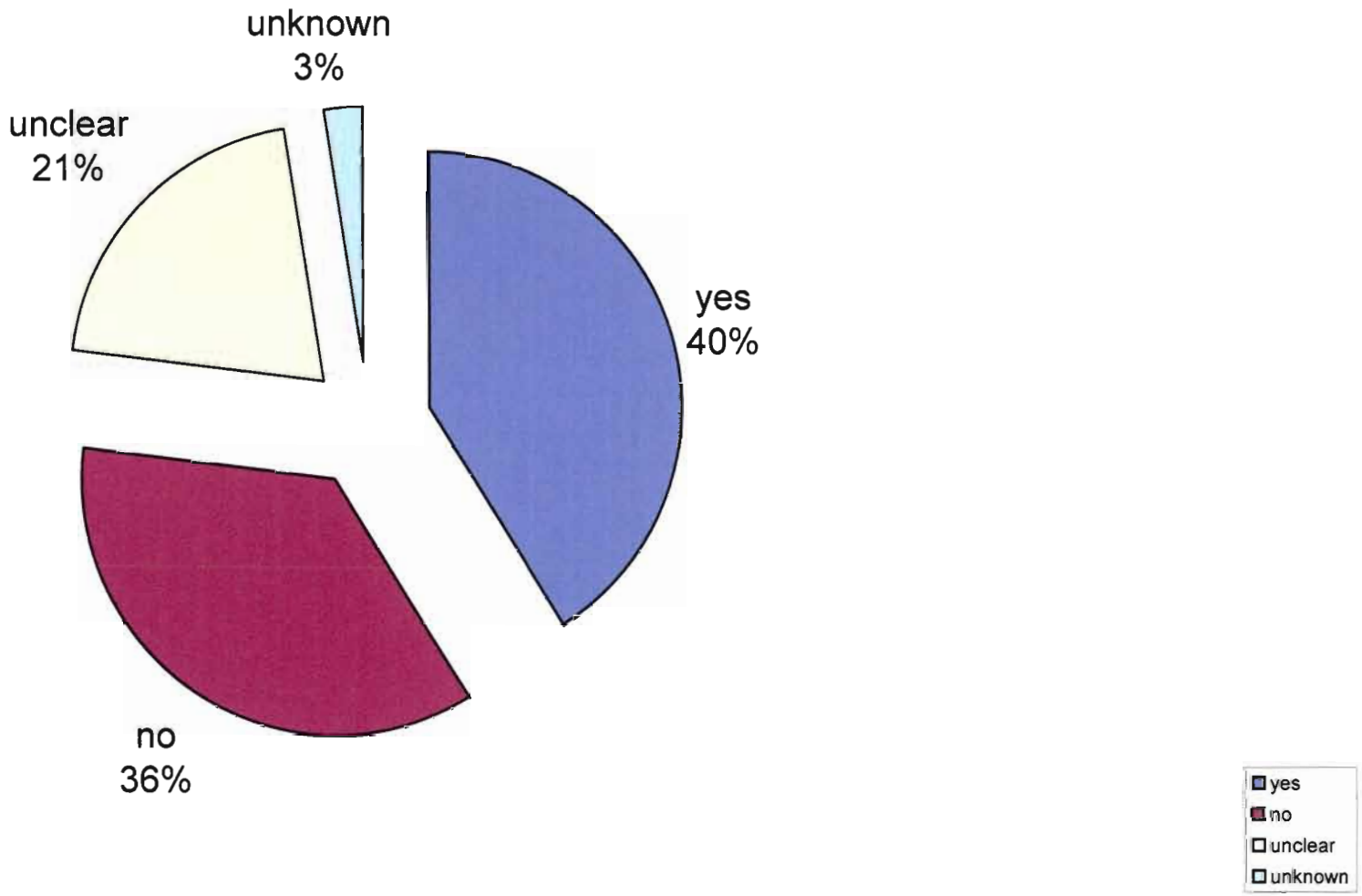

Telephone
no
0%
yes
100%
yes
no

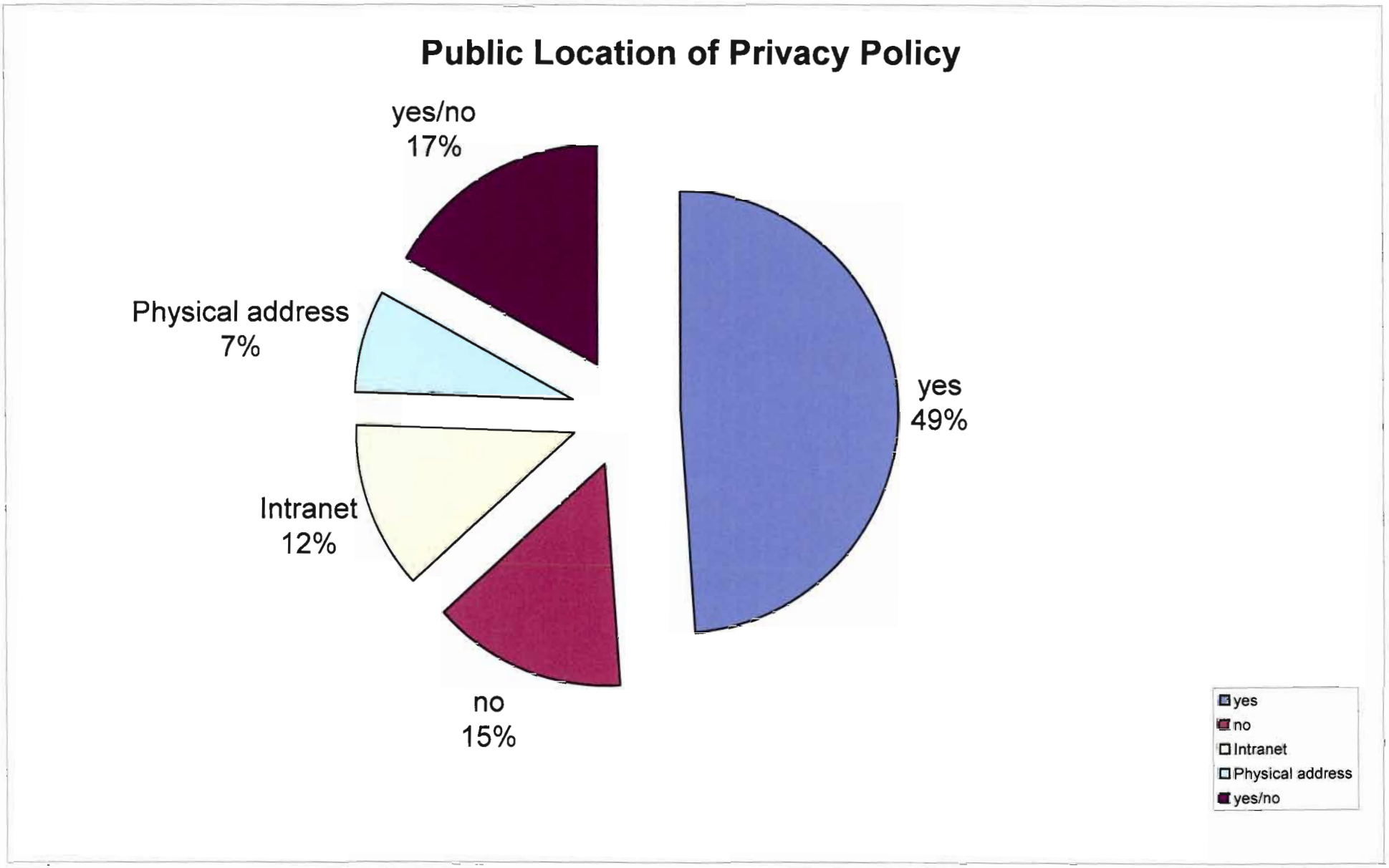
Fax




email
no
0%
yes
100%
yes
no

Description of Types of Processed EU Data




Public Location of Privacy Policy
yes/no
17%
Physical address
7%
Intranet
12%
no
15%
yes
49%
yes
no
Intranet
Physical address
yes/no

Accurate location

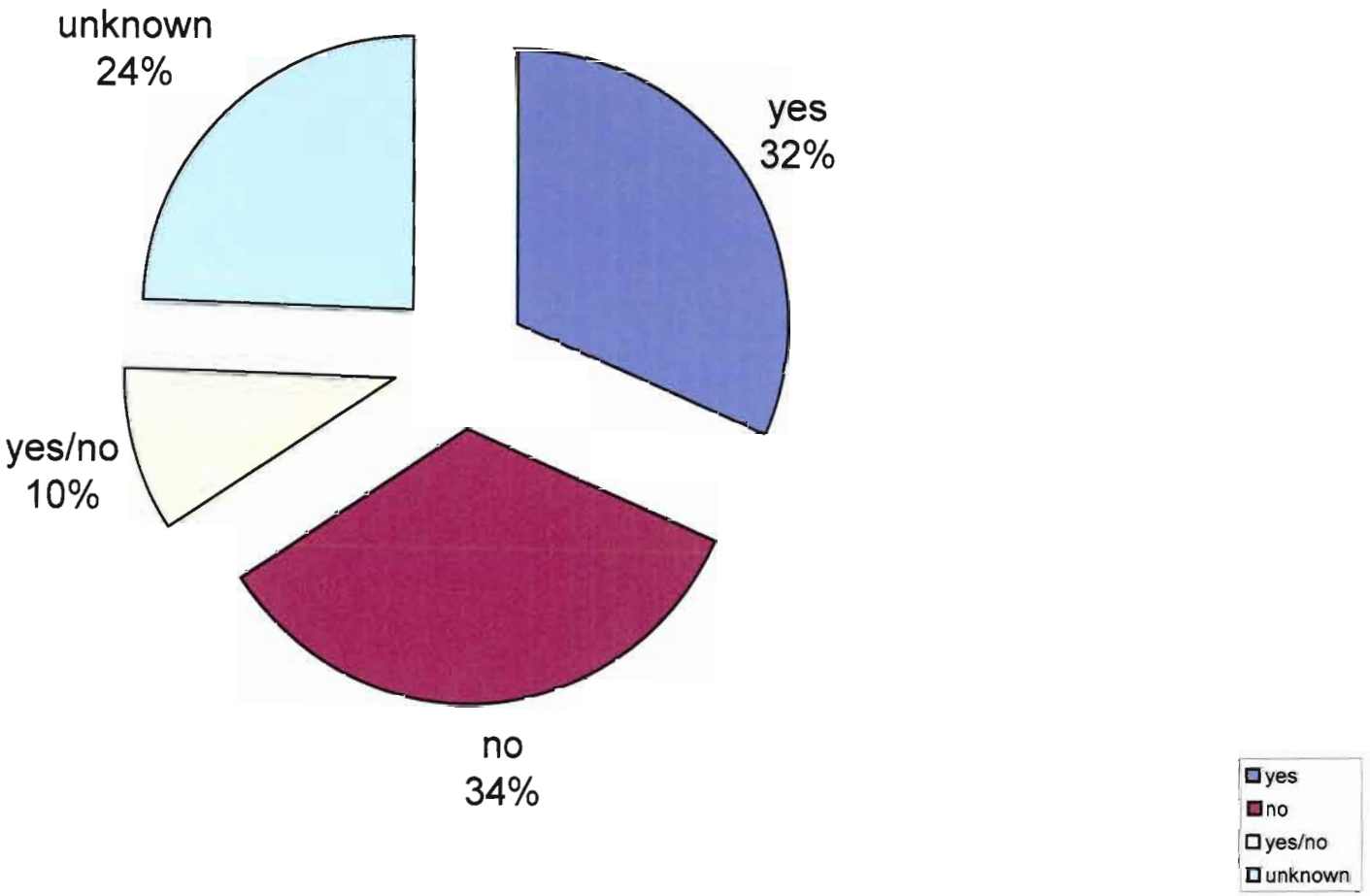
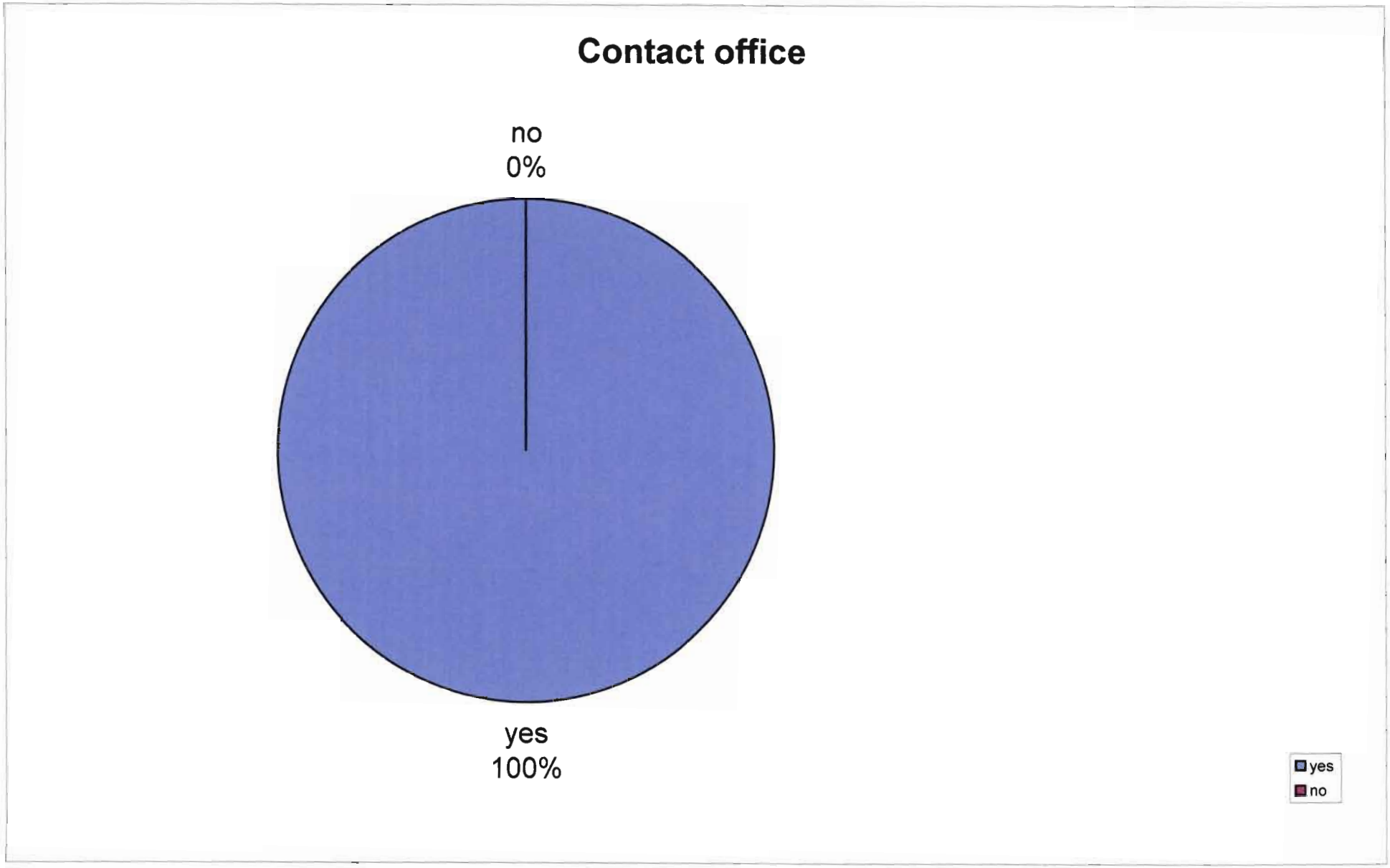
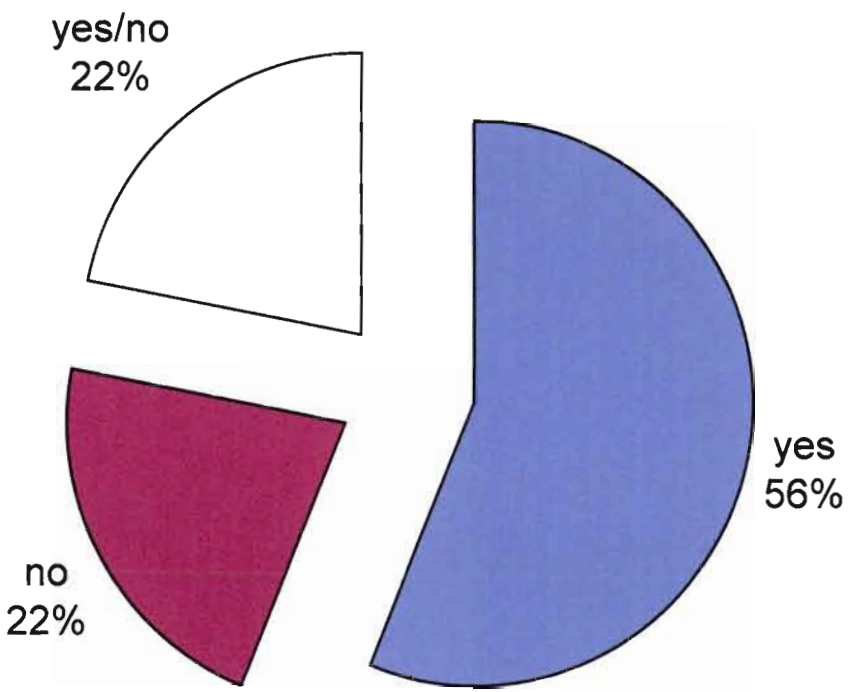


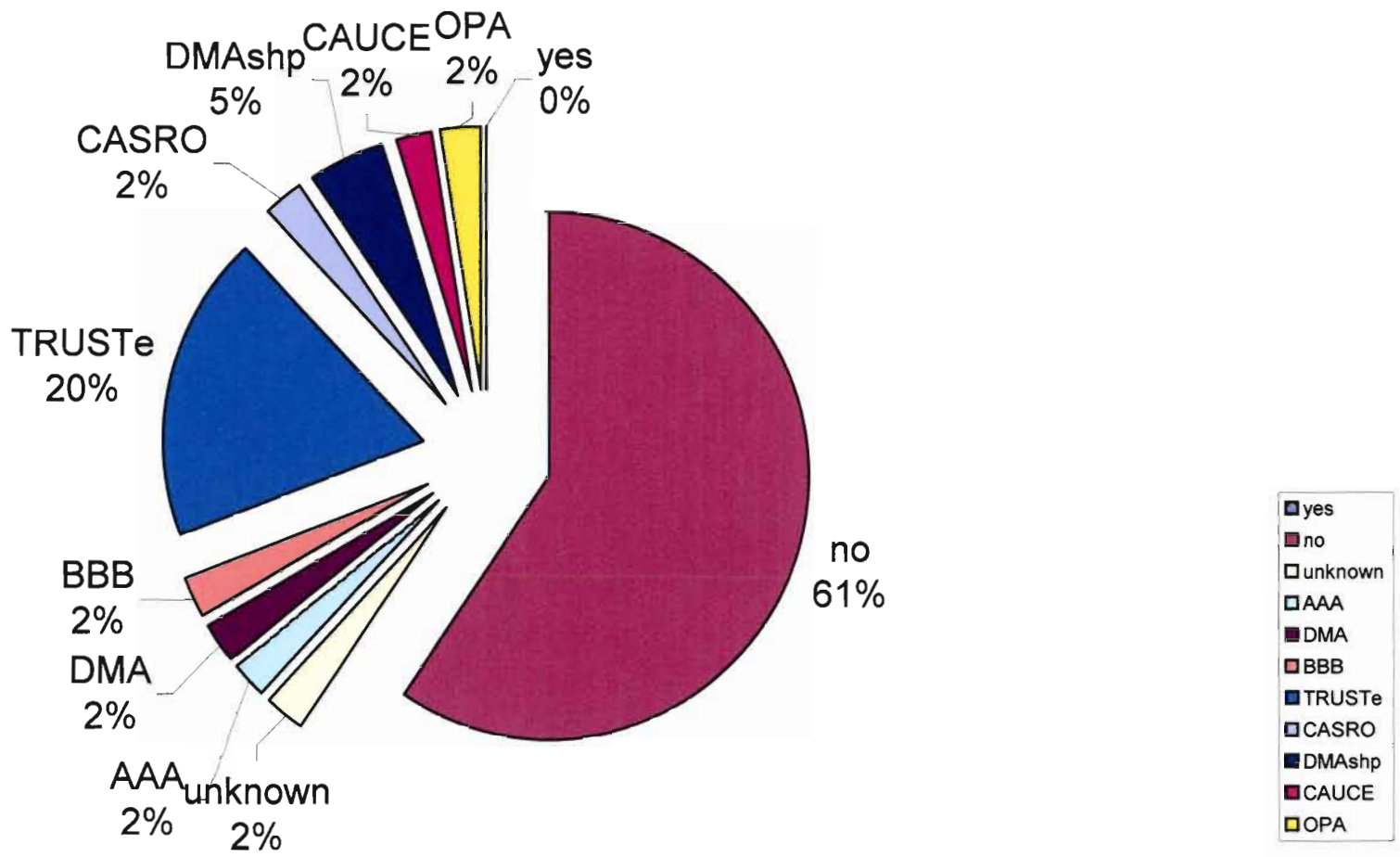
Table 1.3


Contact office
no
0%
yes
100%
yes
no

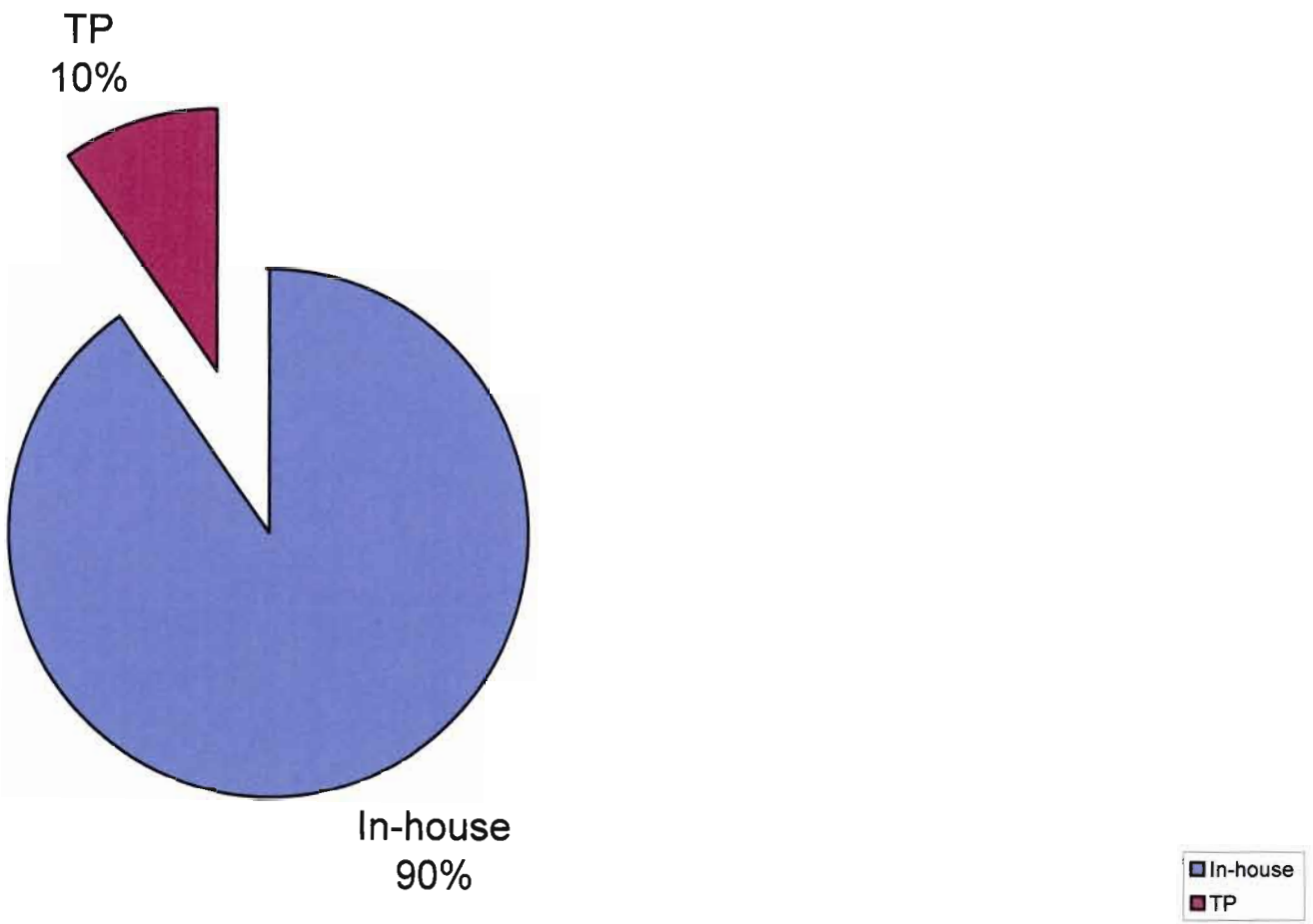
Regulatory Agency



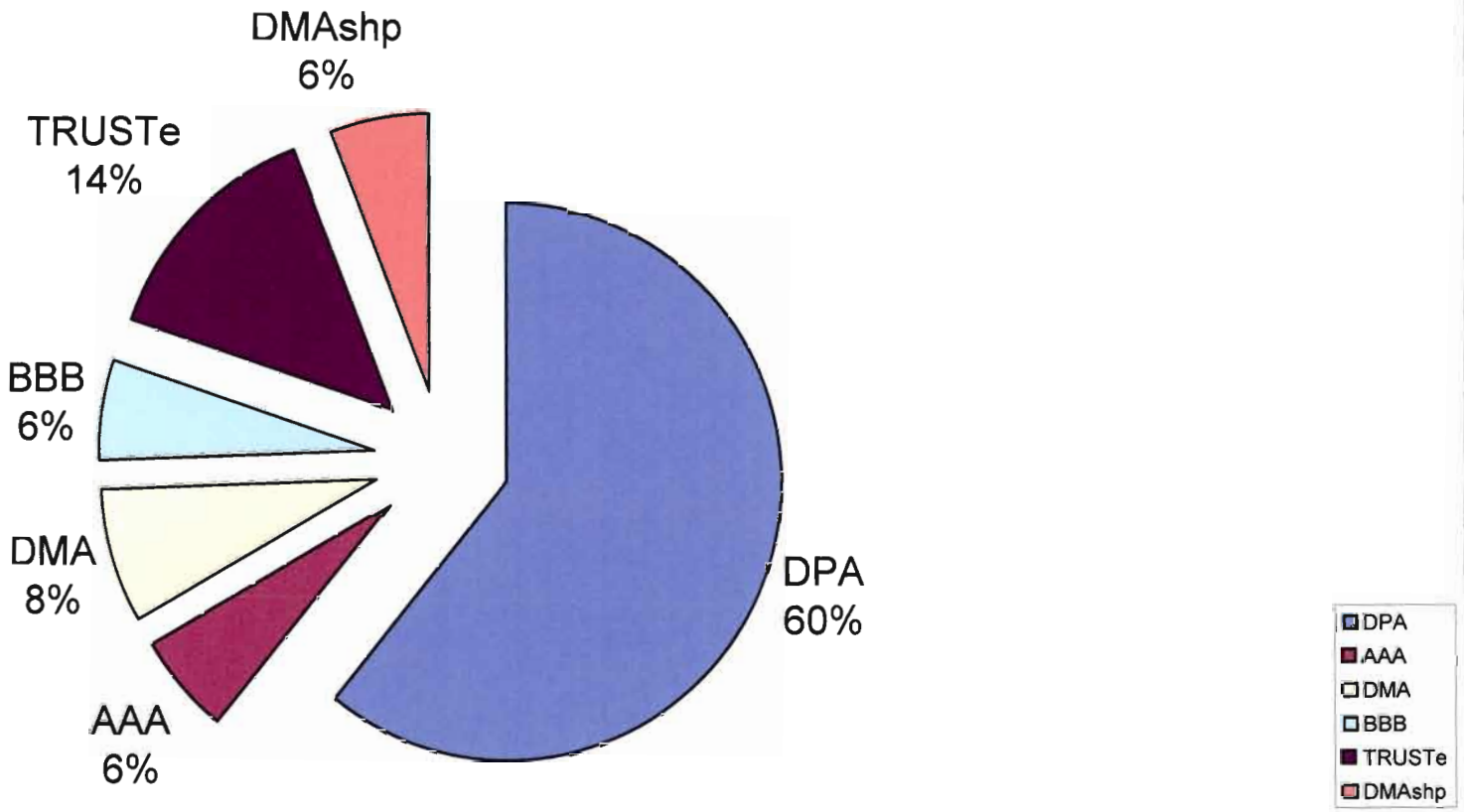
Privacy Program Membership



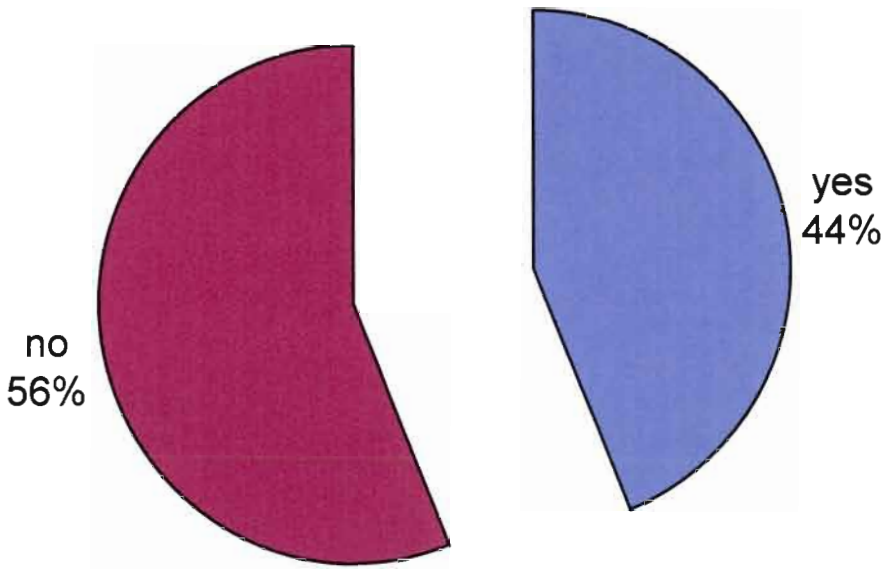
Verification Method



Independent Recourse Mechanism



HR Data



EU Data Coop

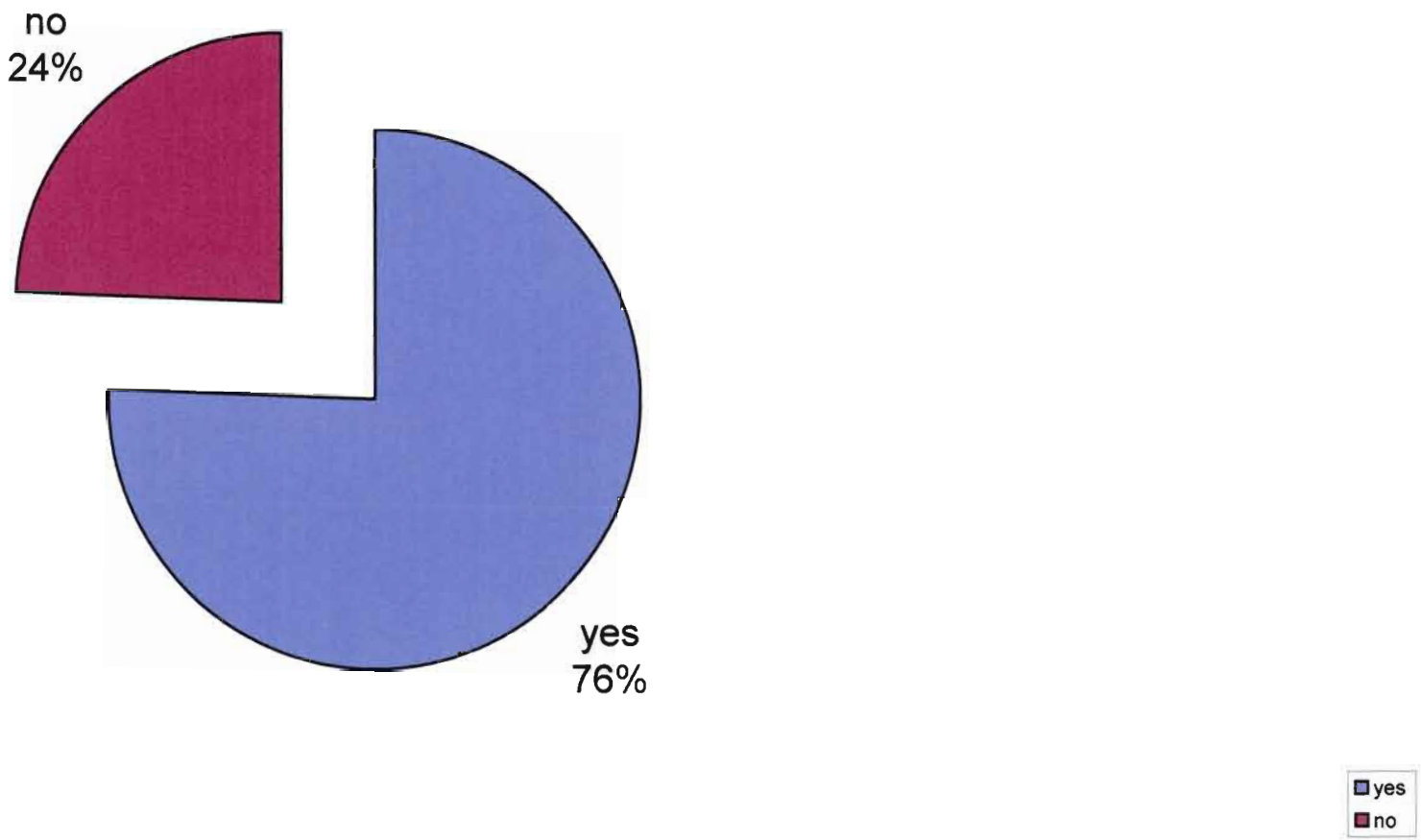
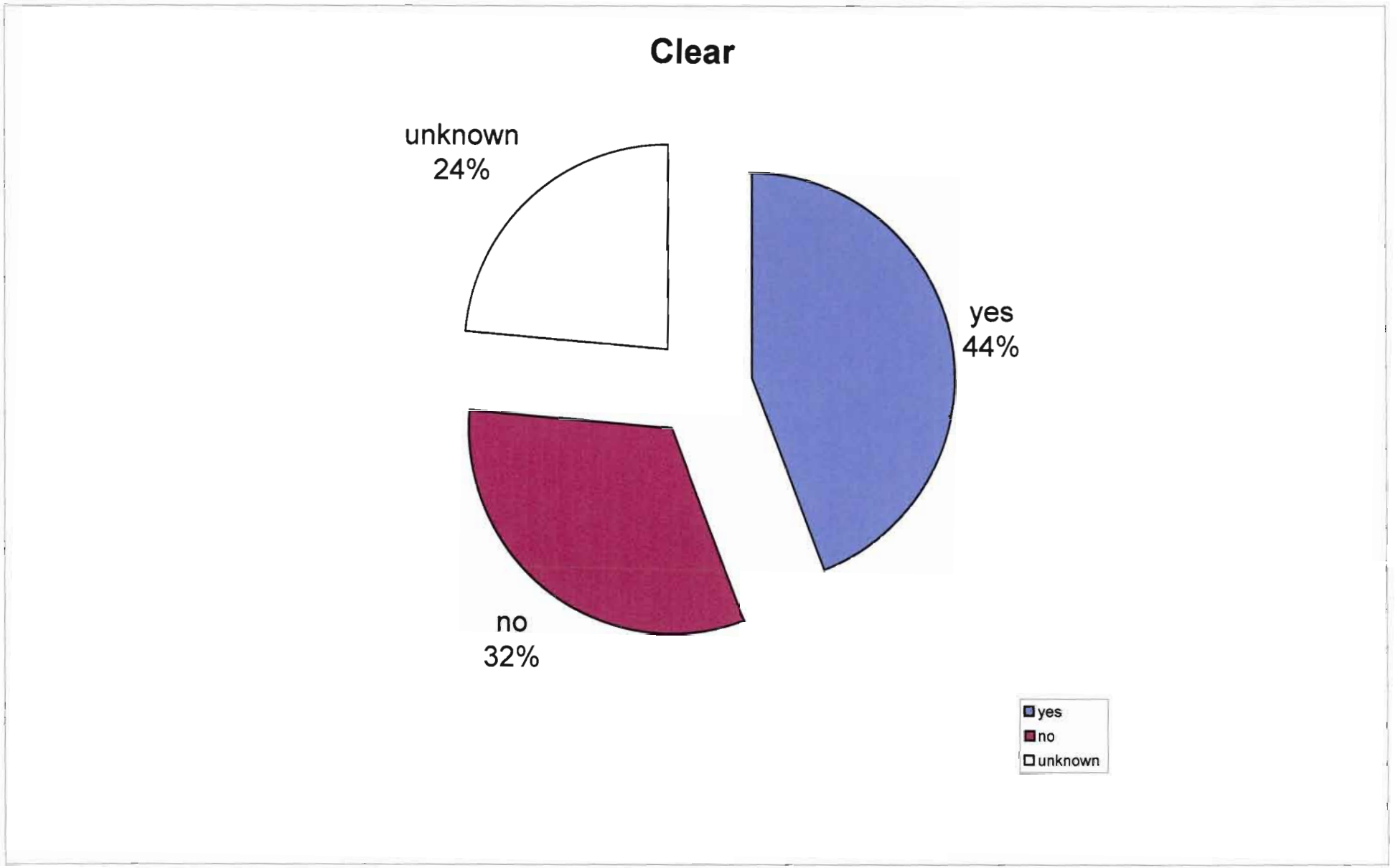
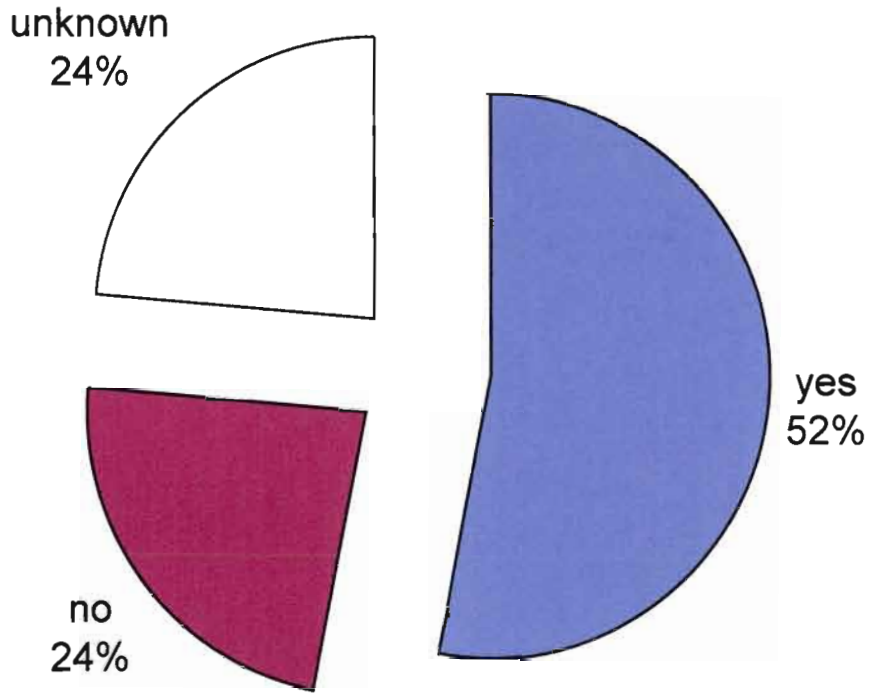
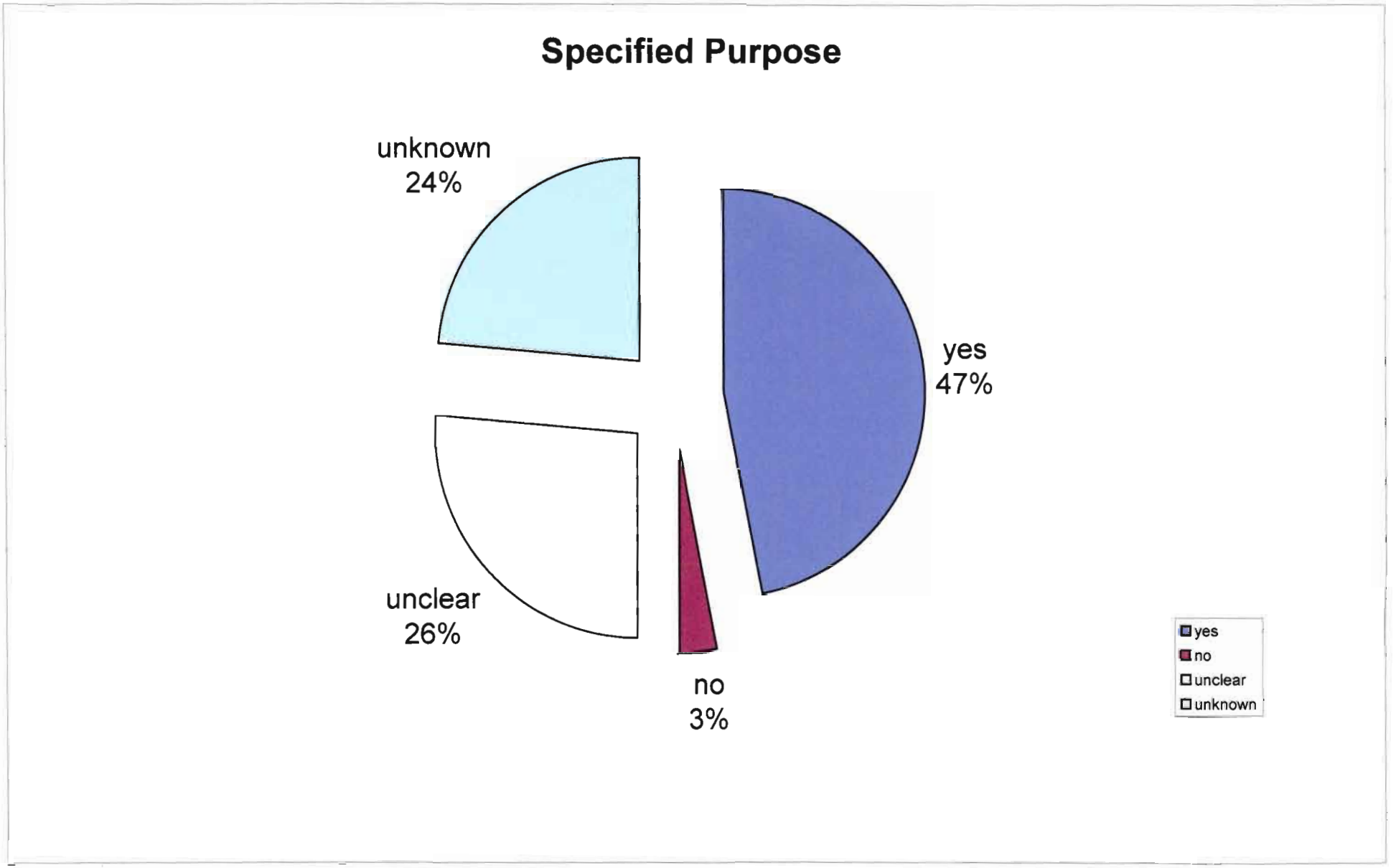


Table 2.1

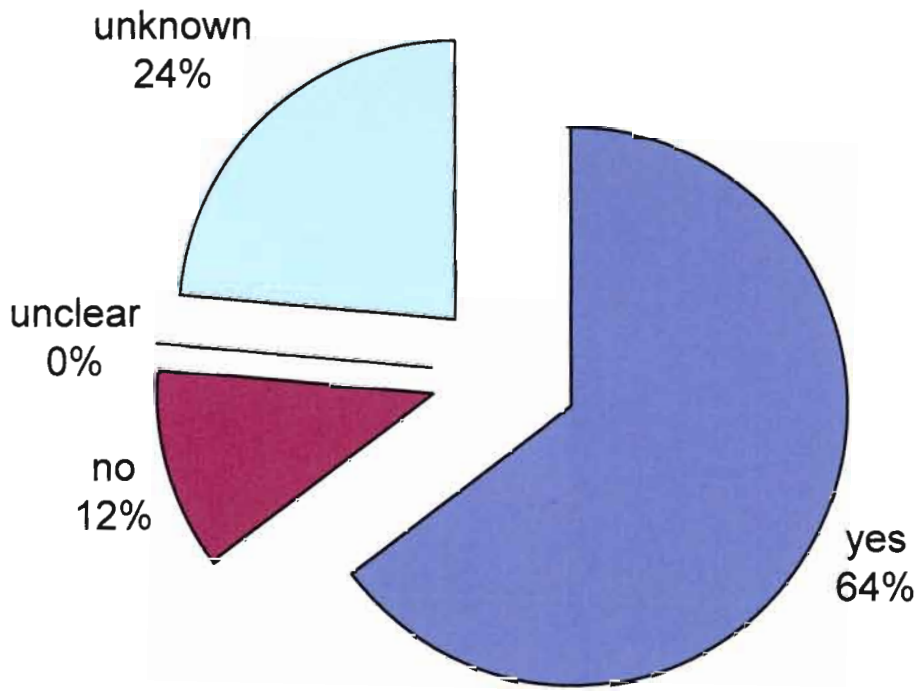

Clear
unknown
24%
yes
44%
no
32%
yes
no
unknown

Conspicuous

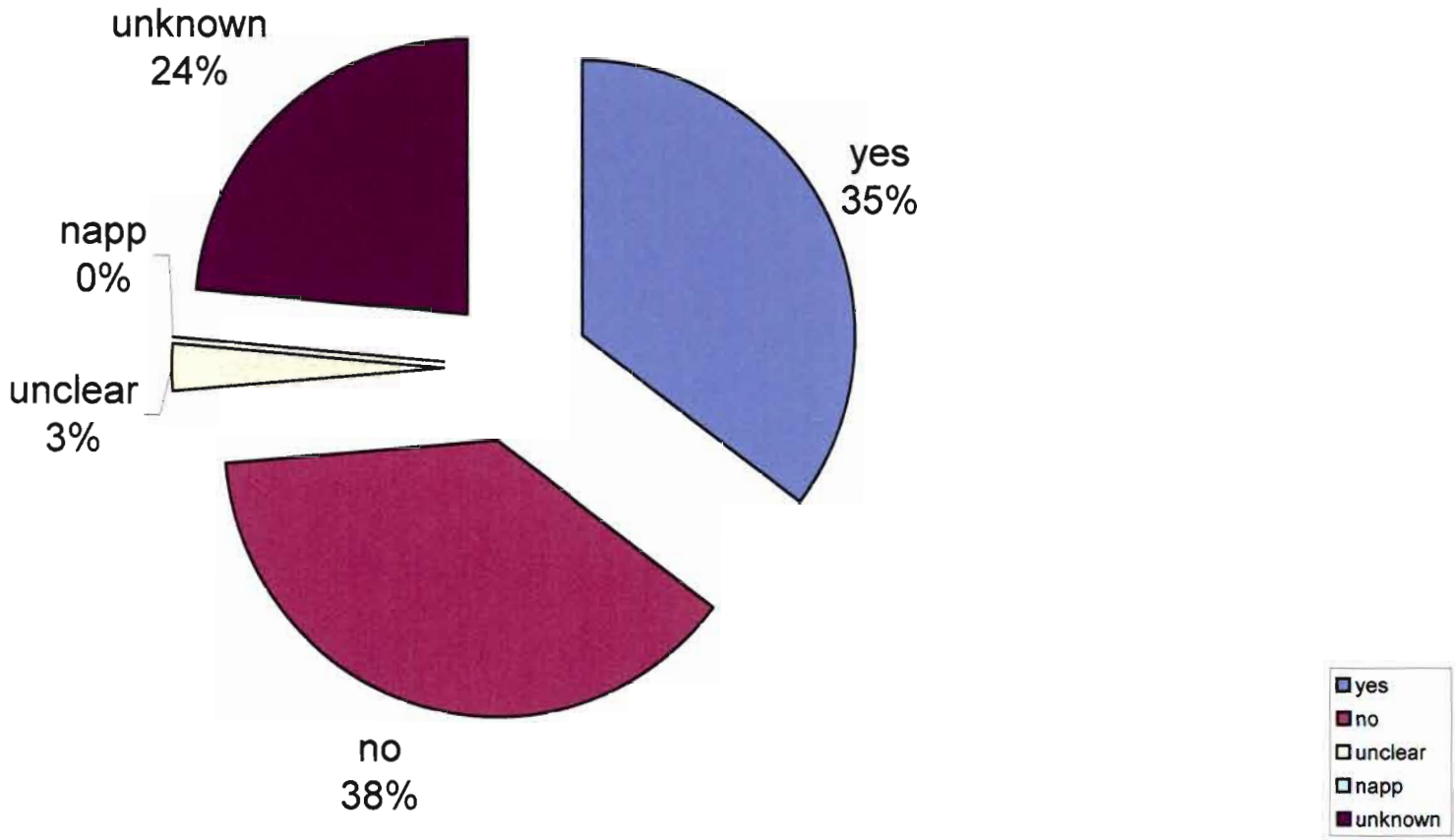



Specified Purpose
unknown
24%
yes
47%
unclear
26%
no
3%
yes
no
unclear
unknown

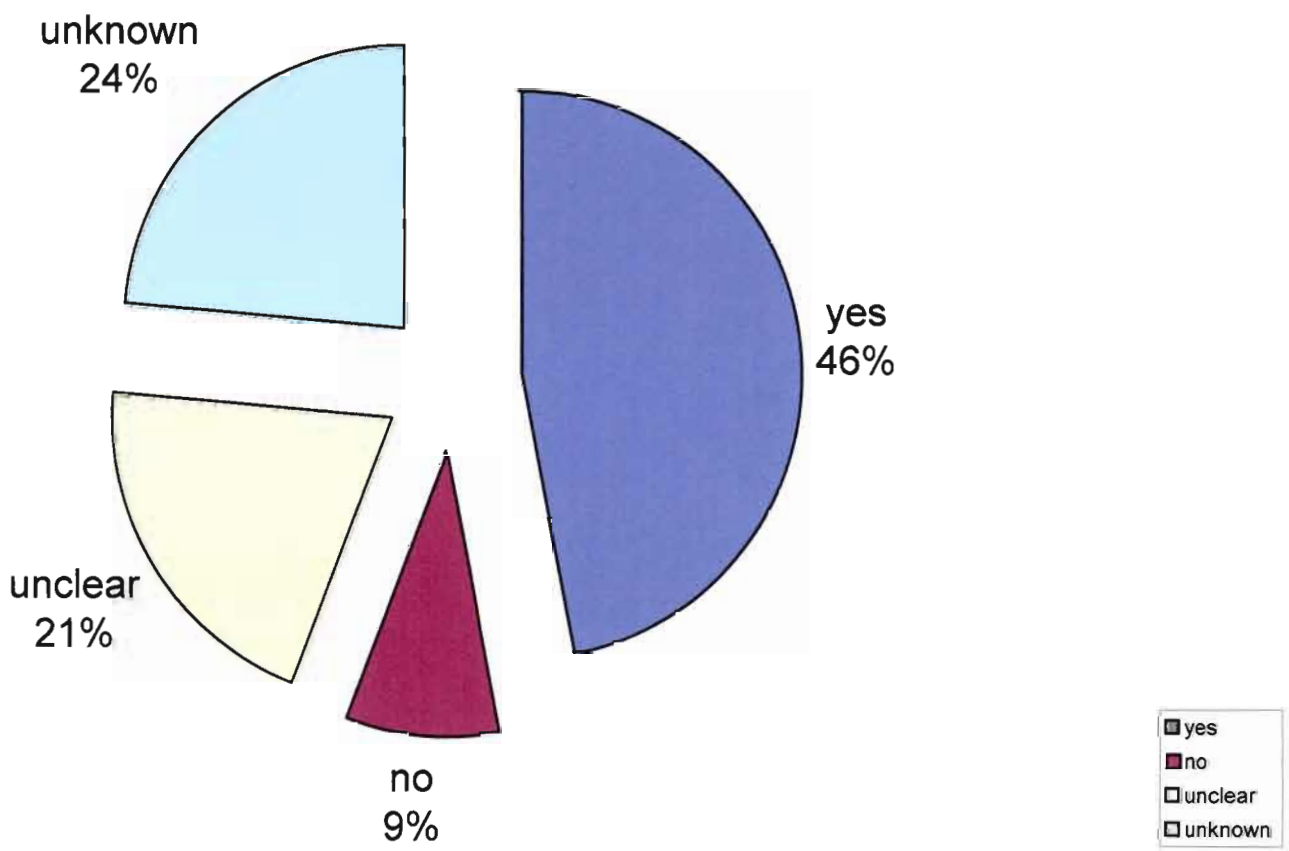
Organization Contacts

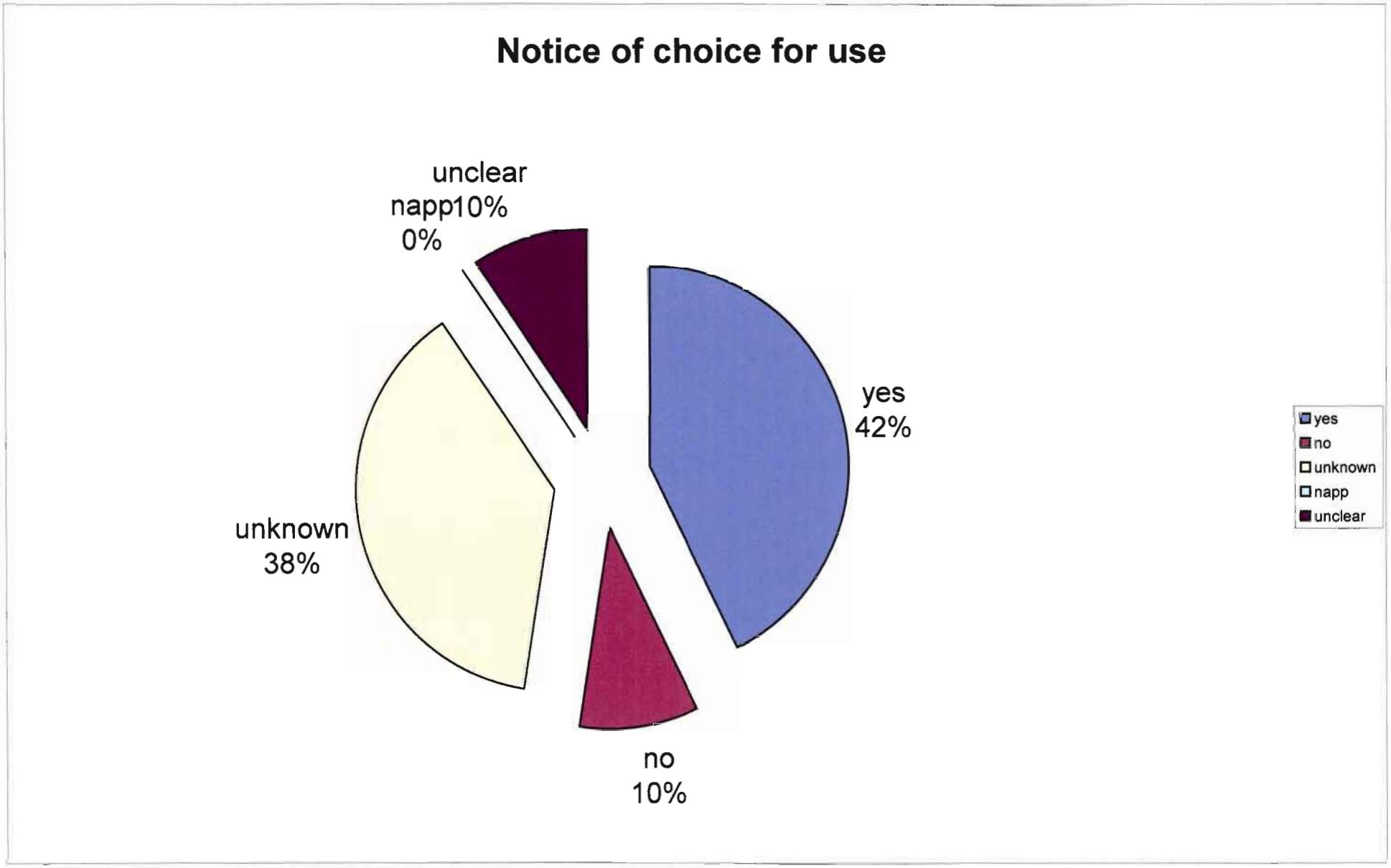


Notice of secondary use

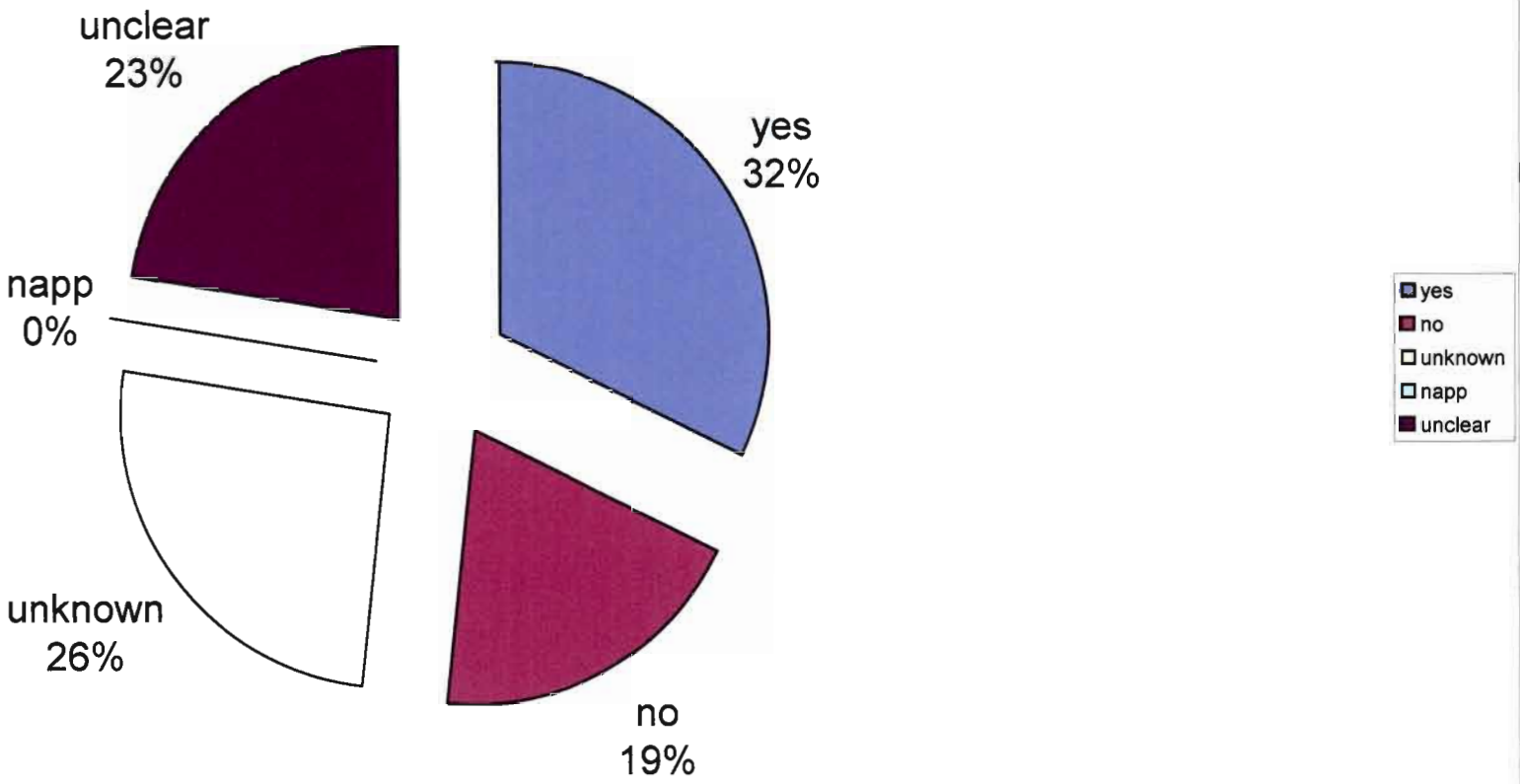


Third Party Disclosures




Notice of choice for use
unclear
napp10%
0%
yes
42%
unknown
38%
no
10%
yes
no
unknown
napp
unclear

Notice of choice for dissemination



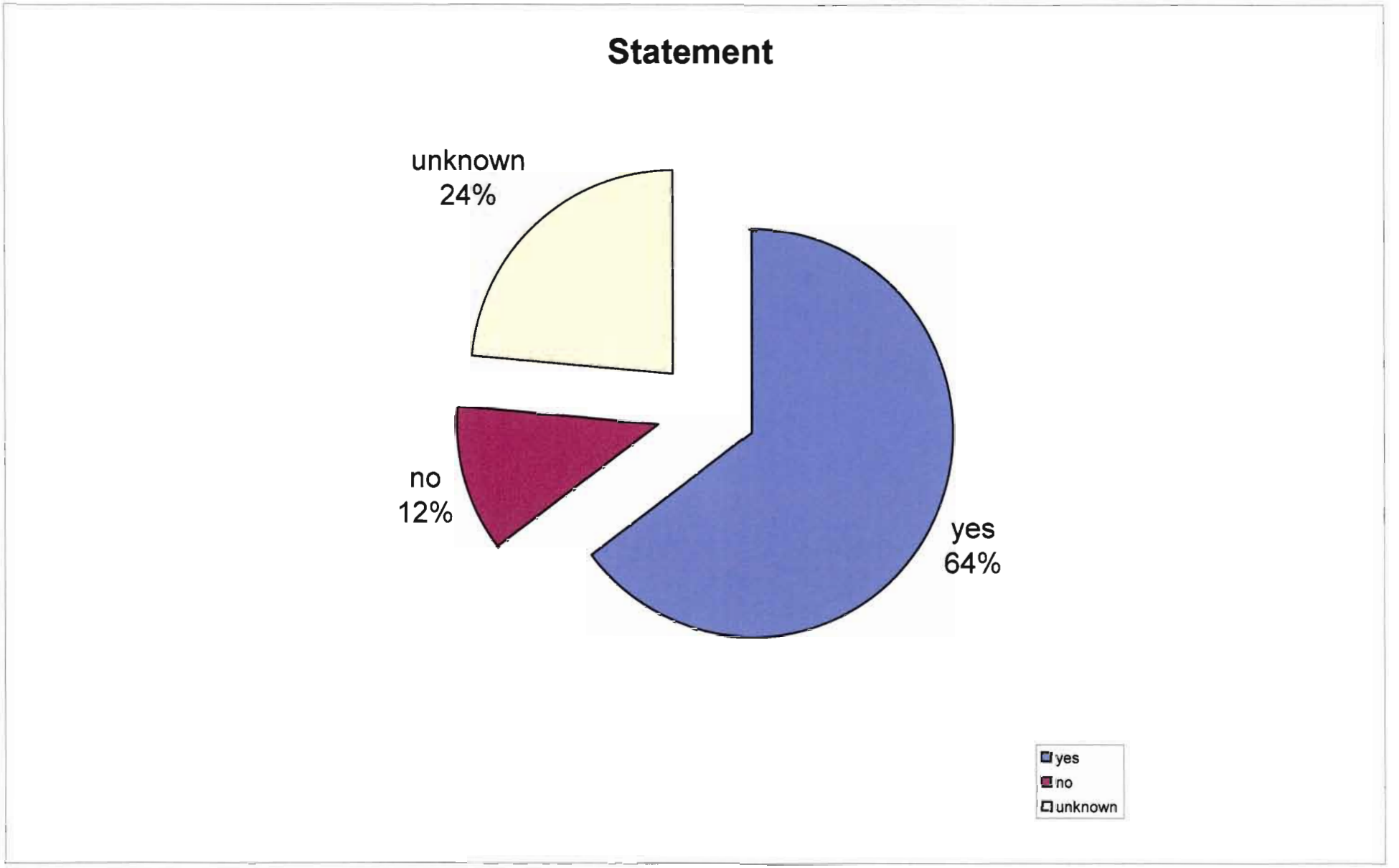
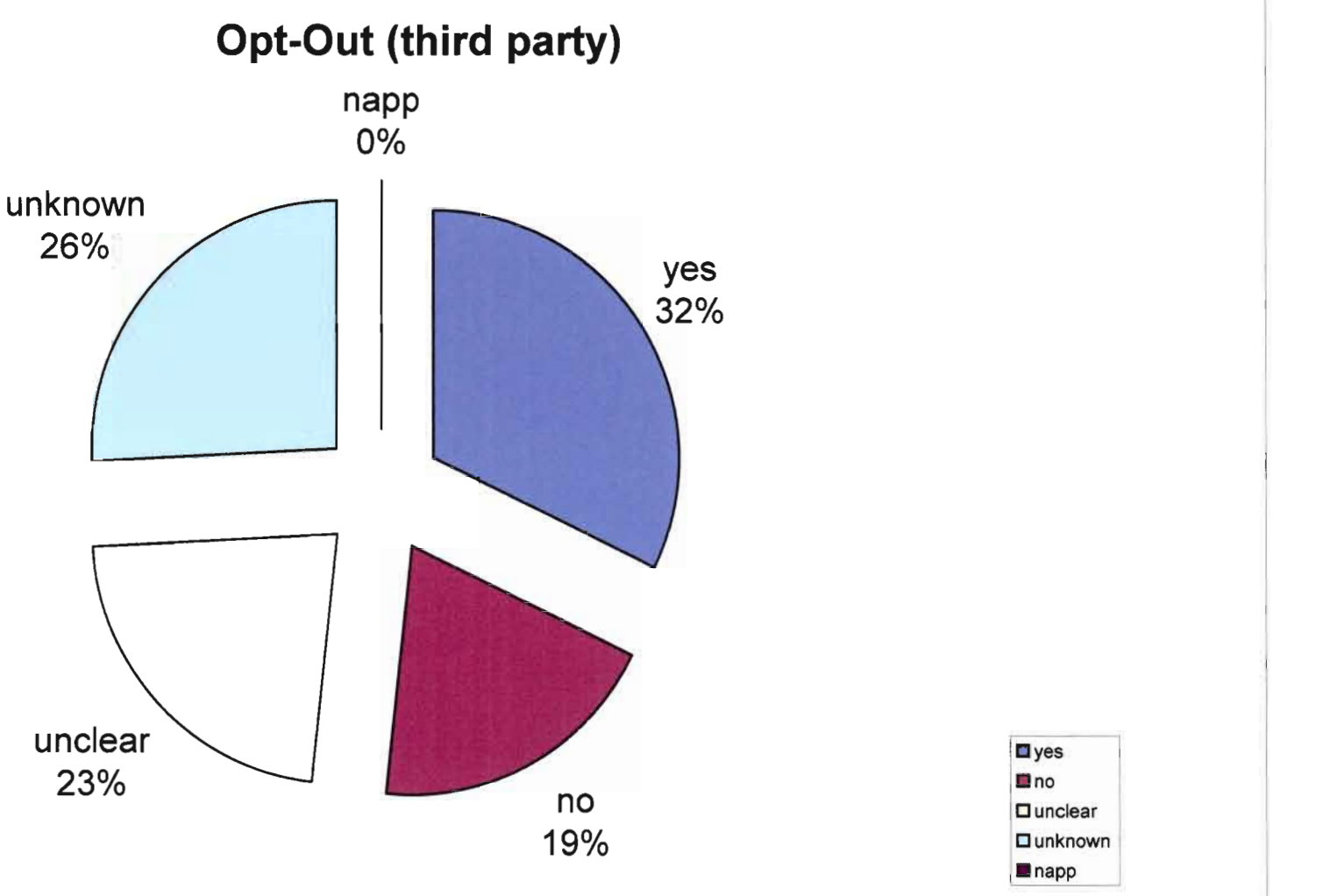
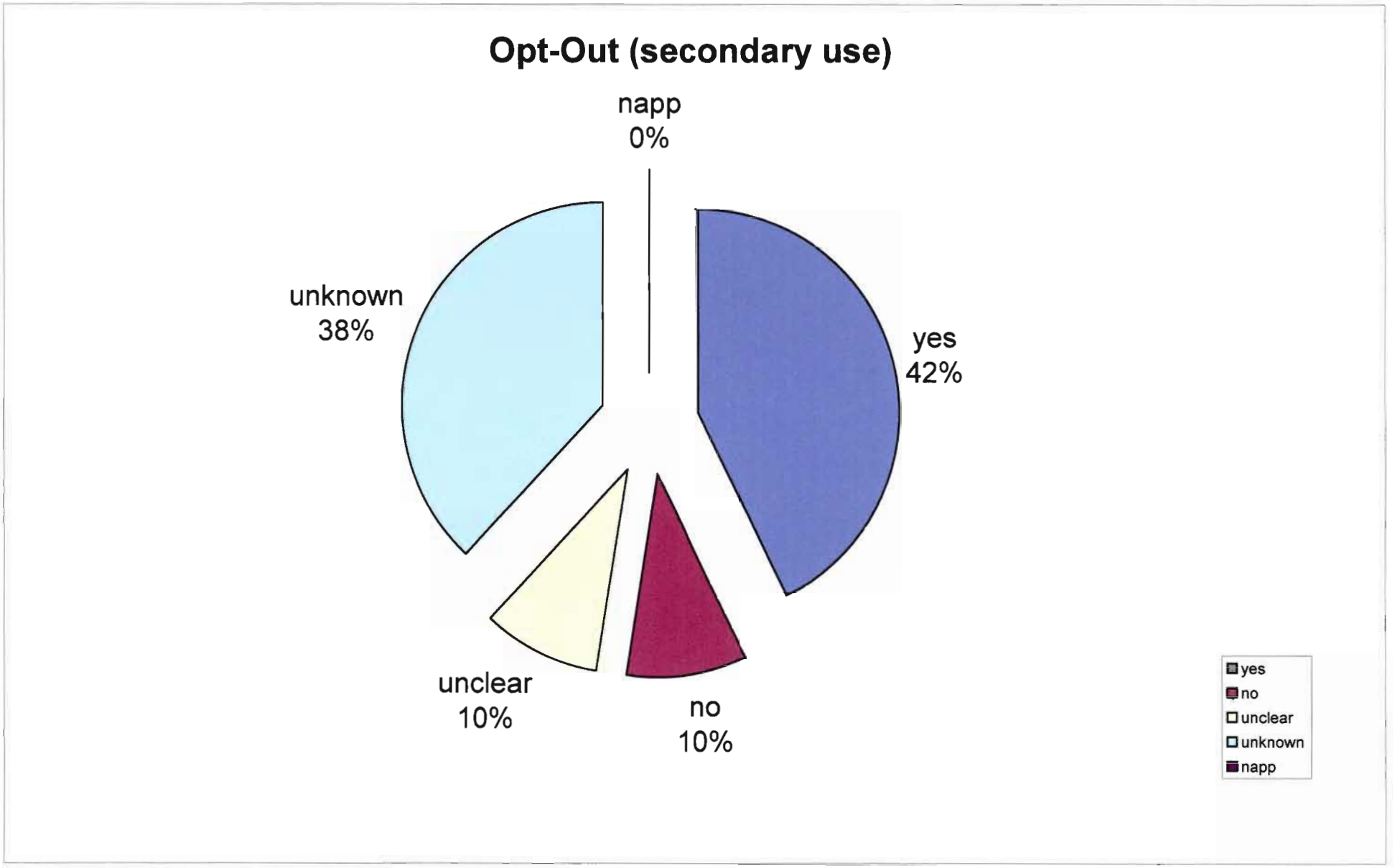
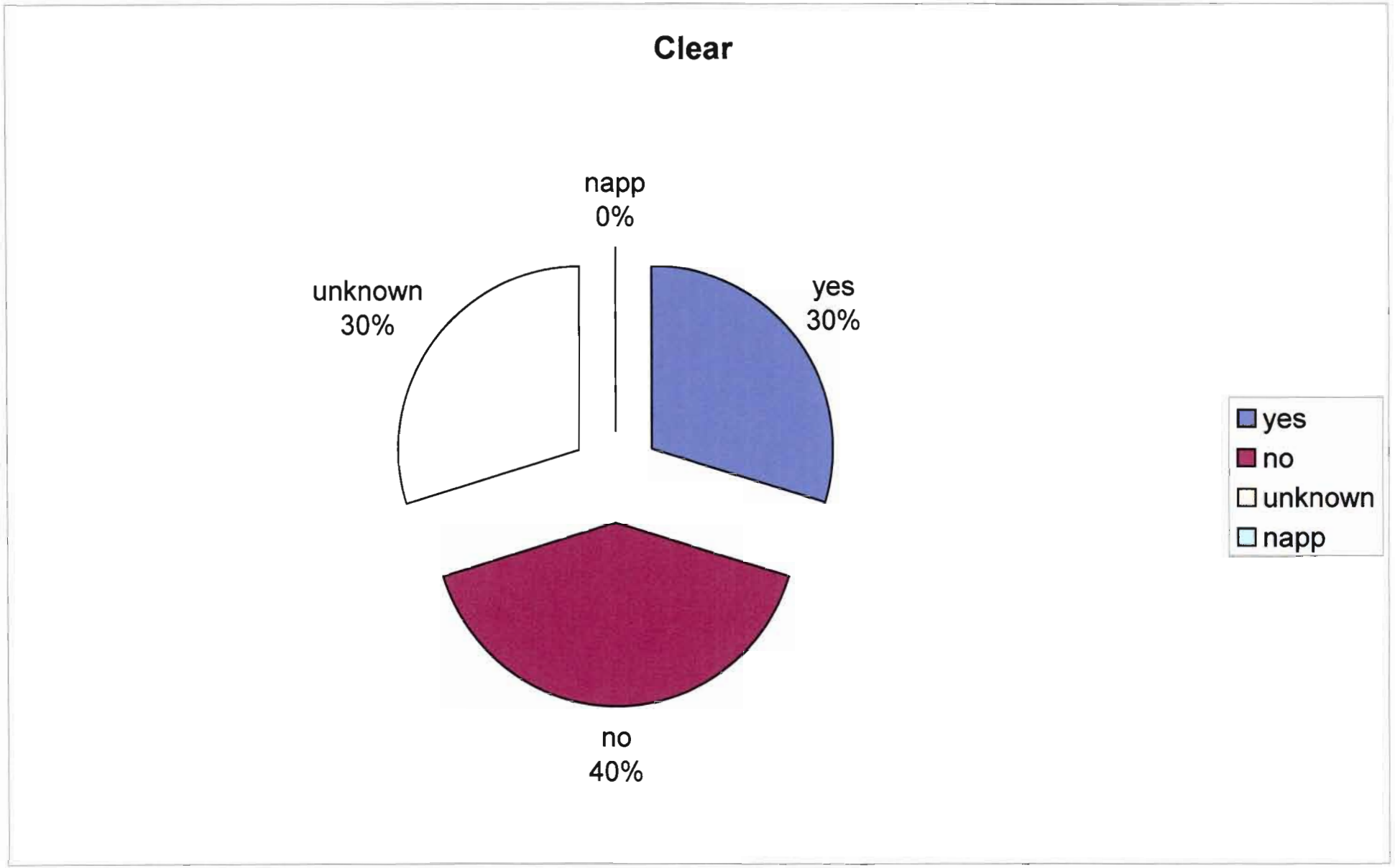
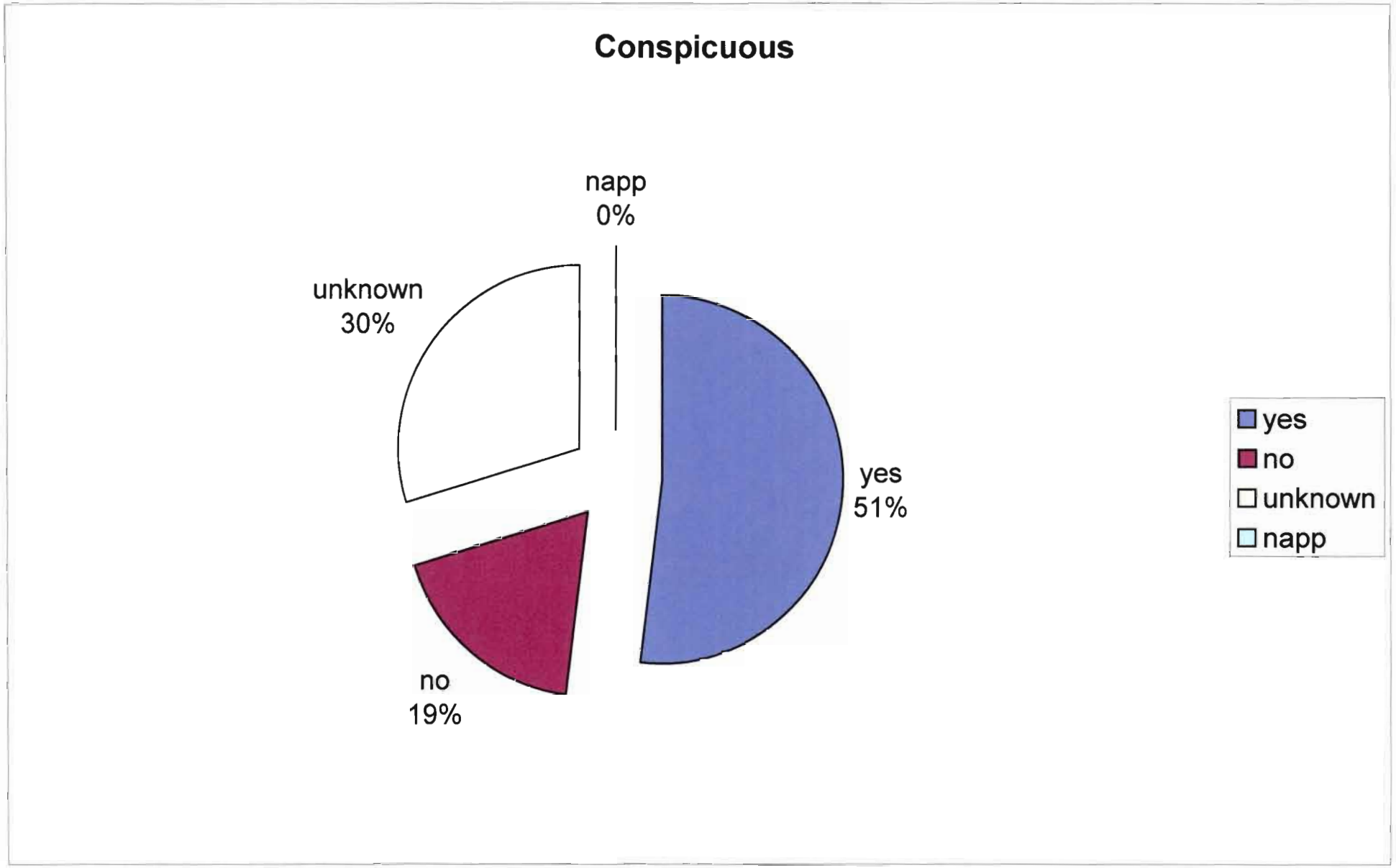

Statement
unknown
24%
no
12%
yes
64%
yes
no
unknown

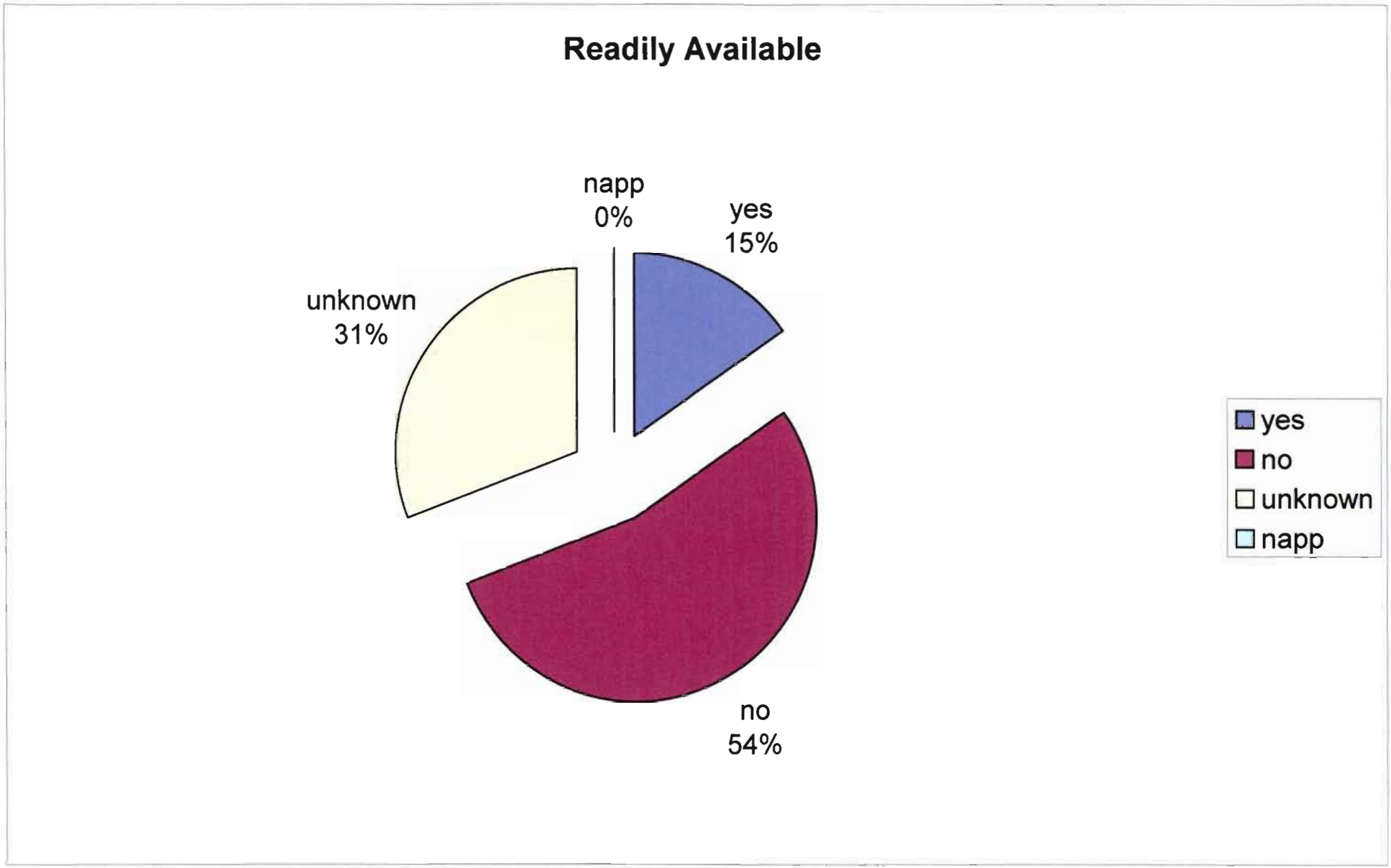
Table 2.2

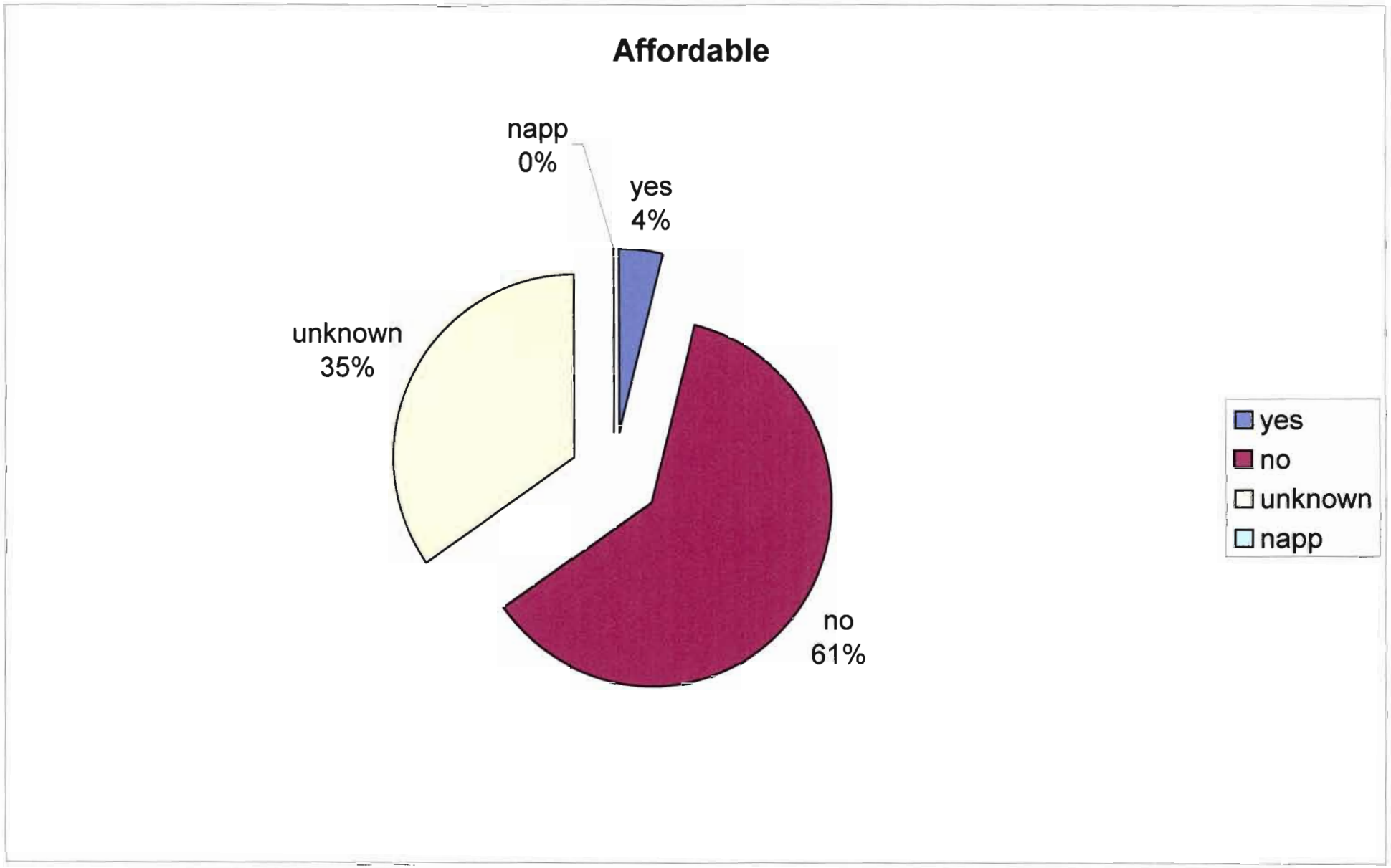

Opt-Out (third party)
napp
0%
unknown
26%
yes
32%
unclear
23%
no
19%
yes
no
unclear
unknown
napp


Opt-Out (secondary use)
napp
0%
unknown
38%
yes
42%
unclear
10%
no
10%
yes
no
unclear
unknown
napp


Clear
napp
0%
unknown
30%
yes
30%
no
40%
yes
no
unknown
napp


Conspicuous
napp
0%
unknown
30%
yes
51%
no
19%
yes
no
unknown
napp


Readily Available
napp
0%
yes
15%
unknown
31%
no
54%
yes
no
unknown
napp


Affordable
napp
0%
yes
4%
unknown
35%
no
61%
yes
no
unknown
napp

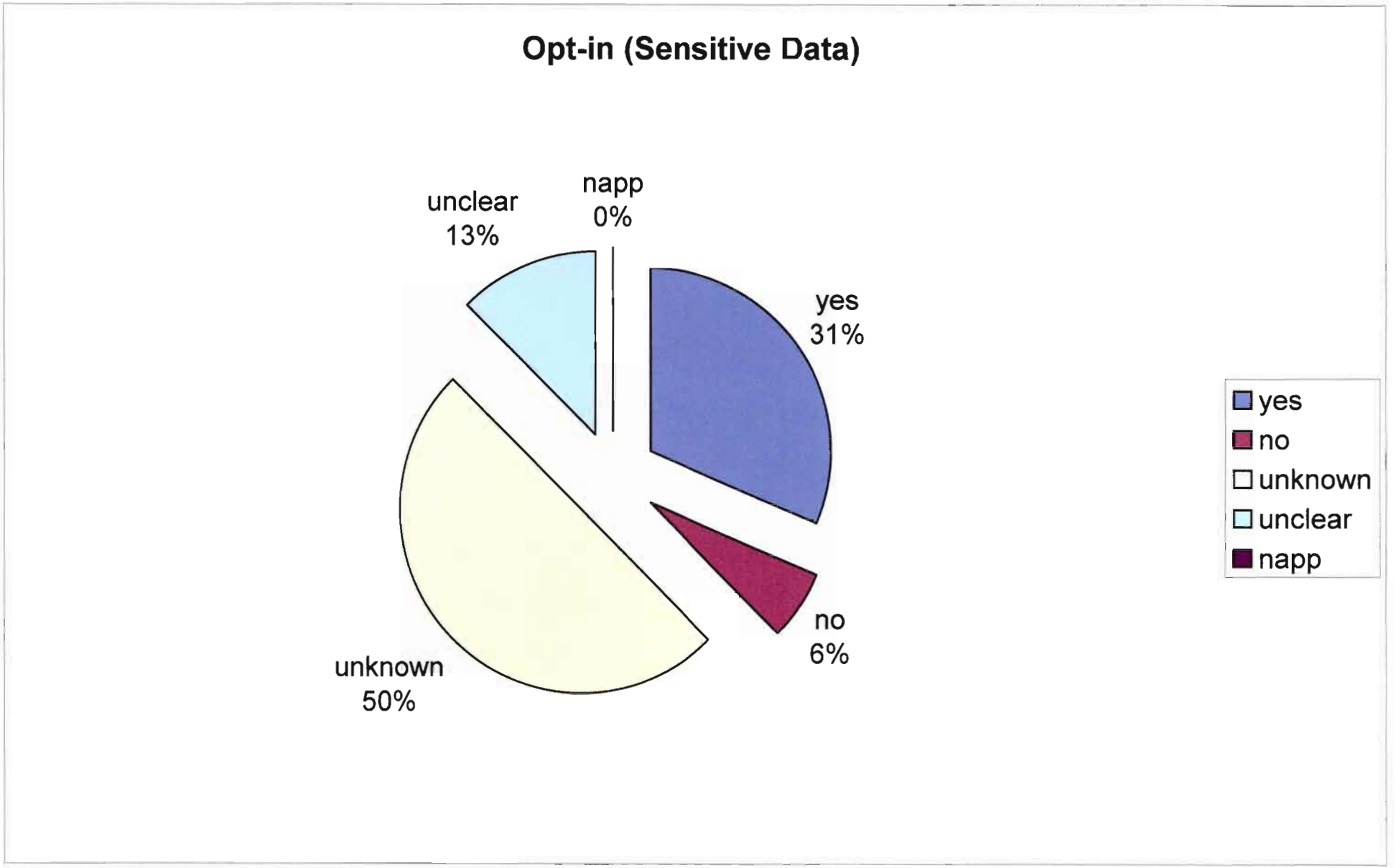
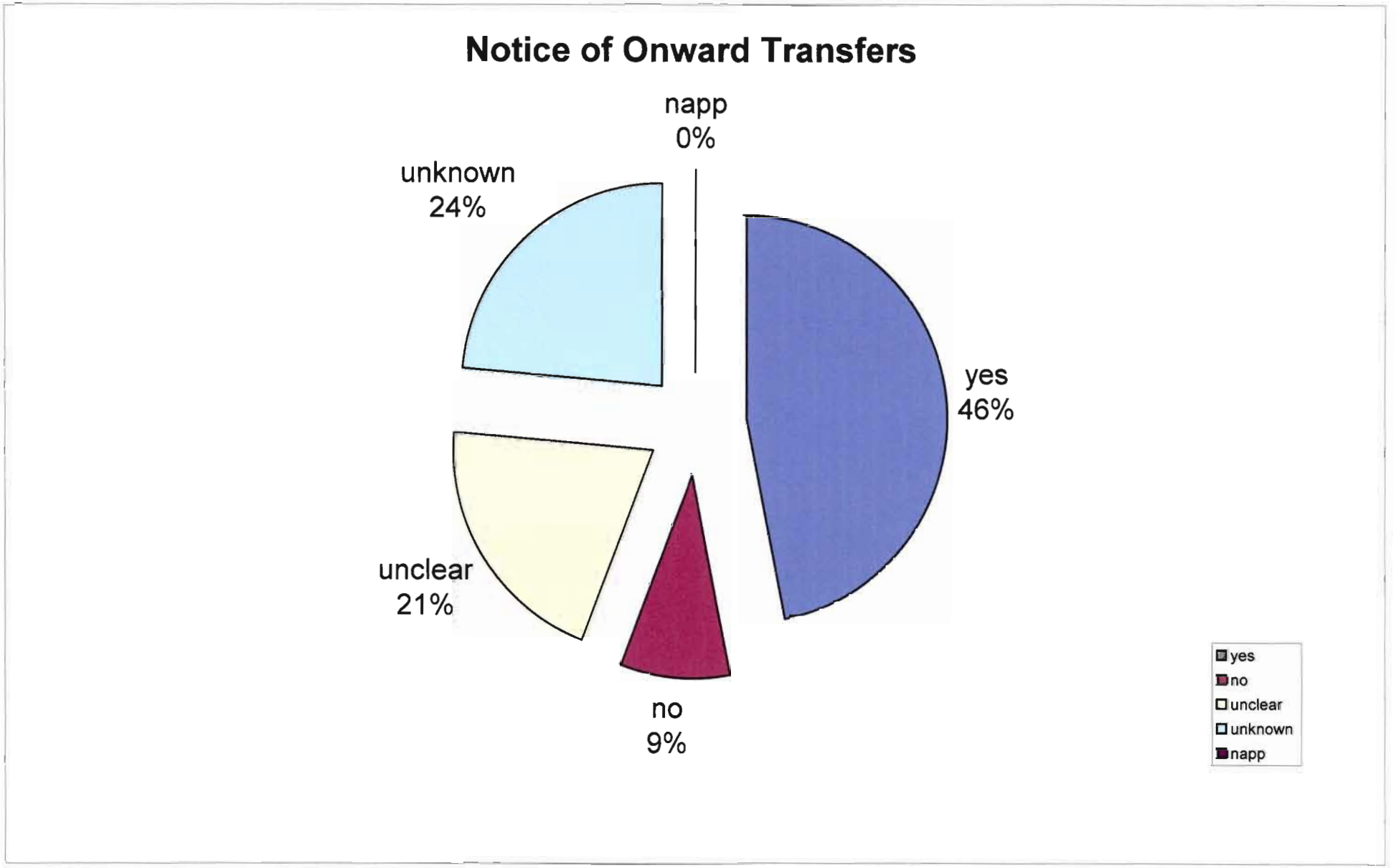
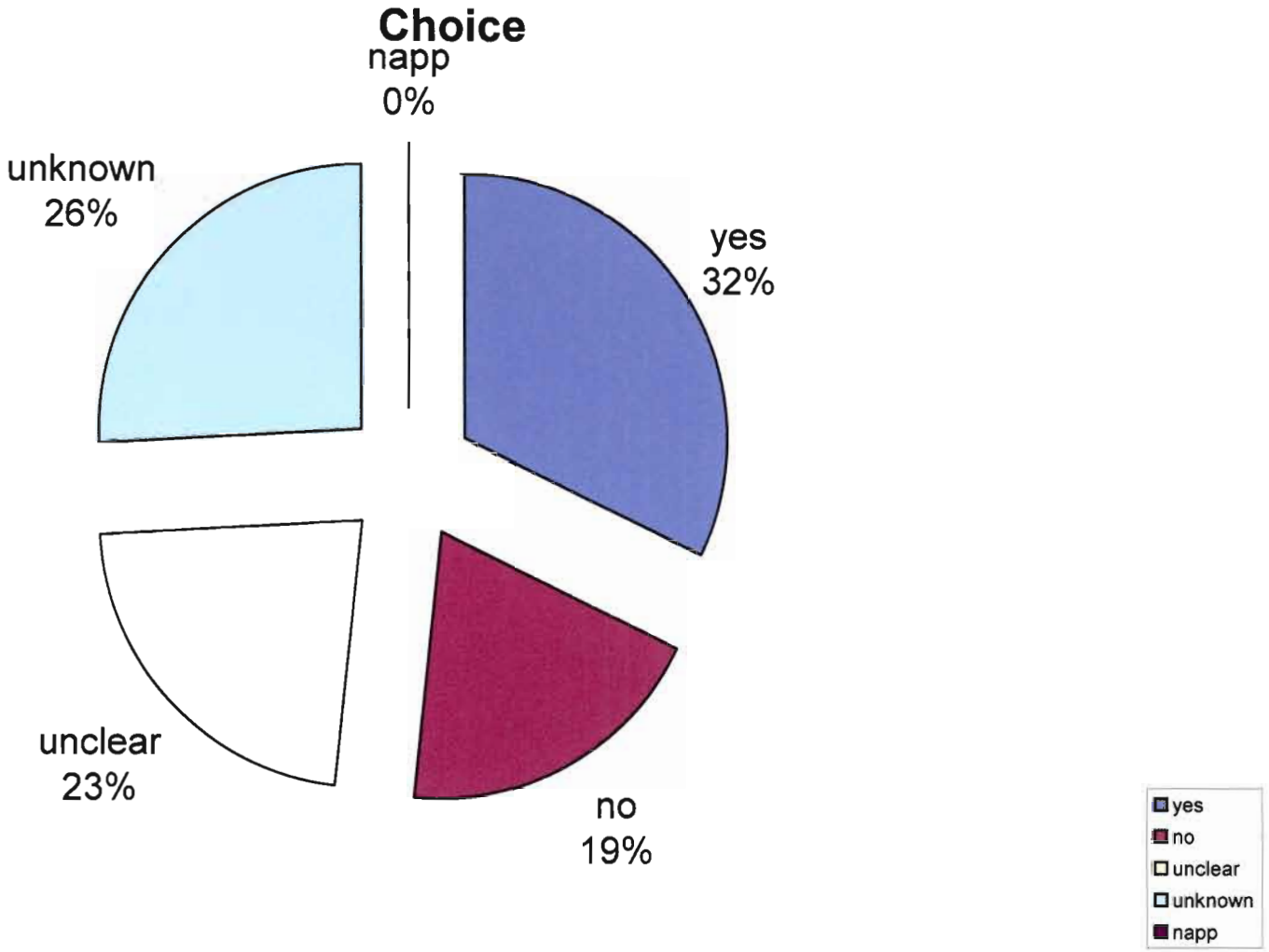

Opt-in (Sensitive Data)
unclear
13%
napp
0%
yes
31%
no
6%
unknown
50%
yes
no
unknown
unclear
napp

Table 2.3


Notice of Onward Transfers
napp
0%
unknown
24%
yes
46%
unclear
21%
no
9%
yes
no
unclear
unknown
napp


Choice
napp
0%
unknown
26%
yes
32%
unclear
23%
no
19%
yes
no
unclear
unknown
napp

Third Party Processor's Commitment to SH

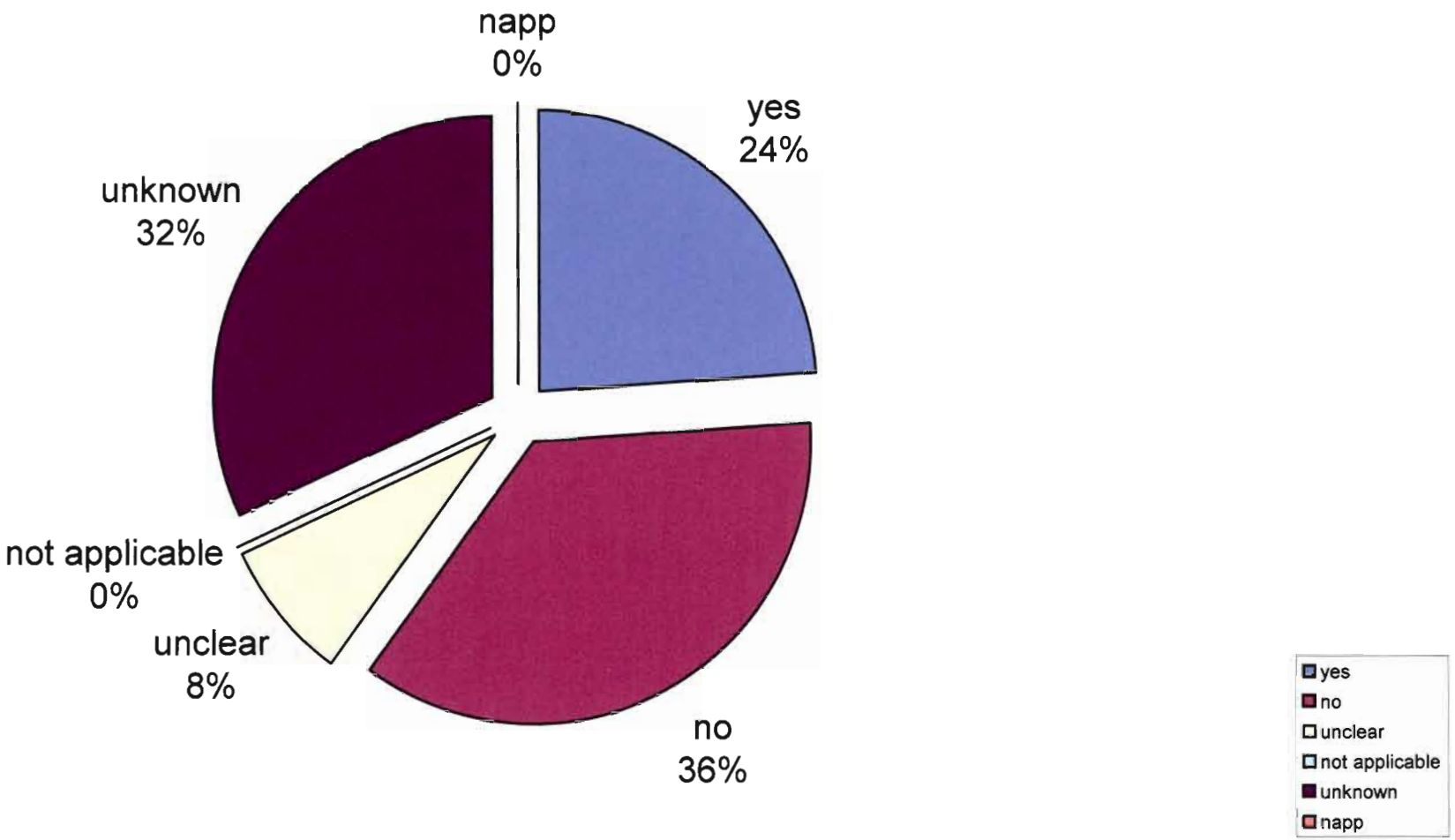
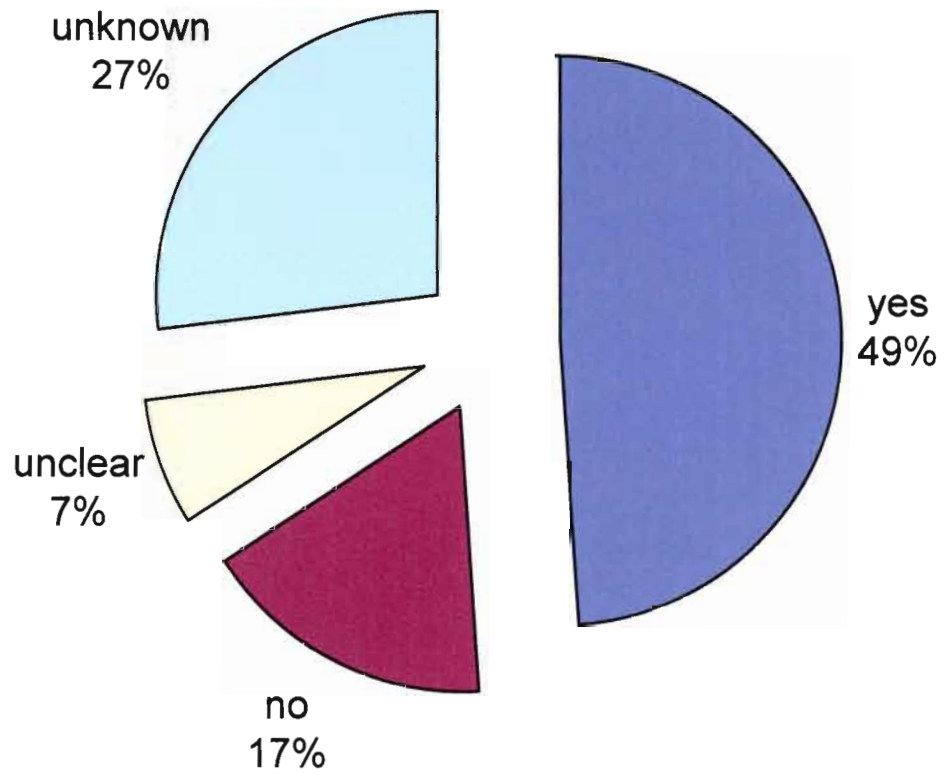
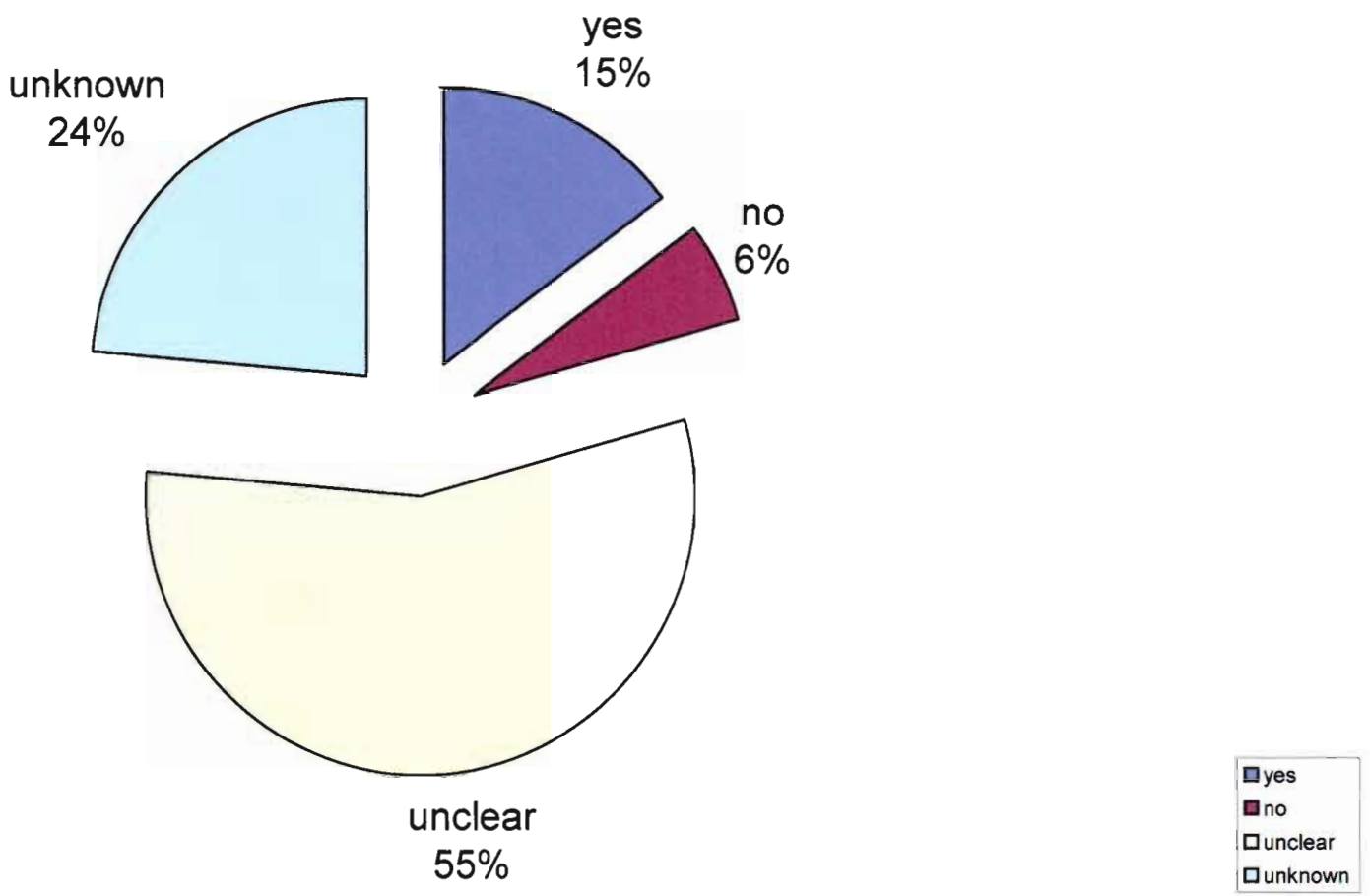


Table 2.4

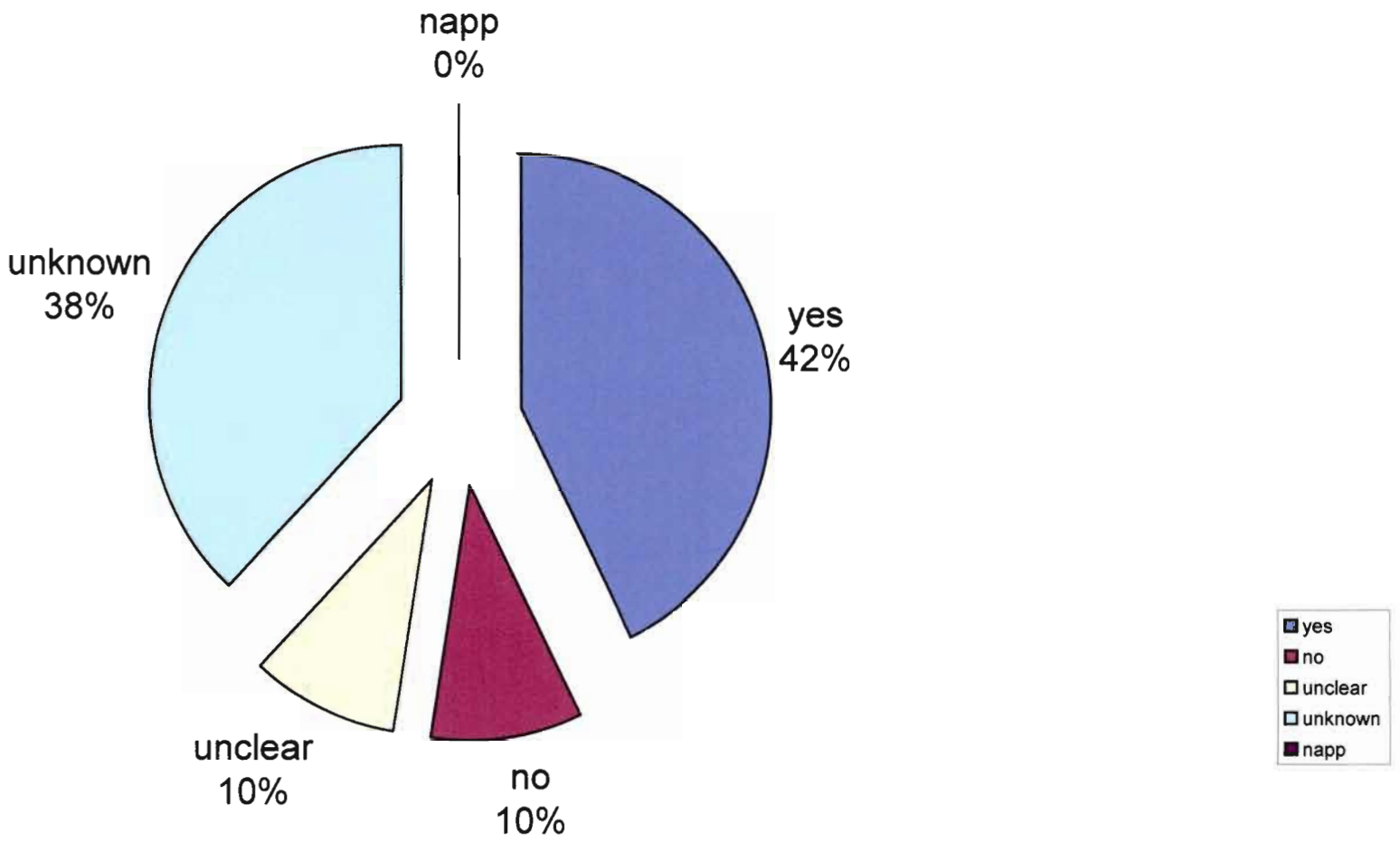
Reasonable Security Precautions



Relevance of Data for Specified Purpose



Compatible/Authorized Processing for Secondary use



Steps to Eunsure Reliability for Intended use

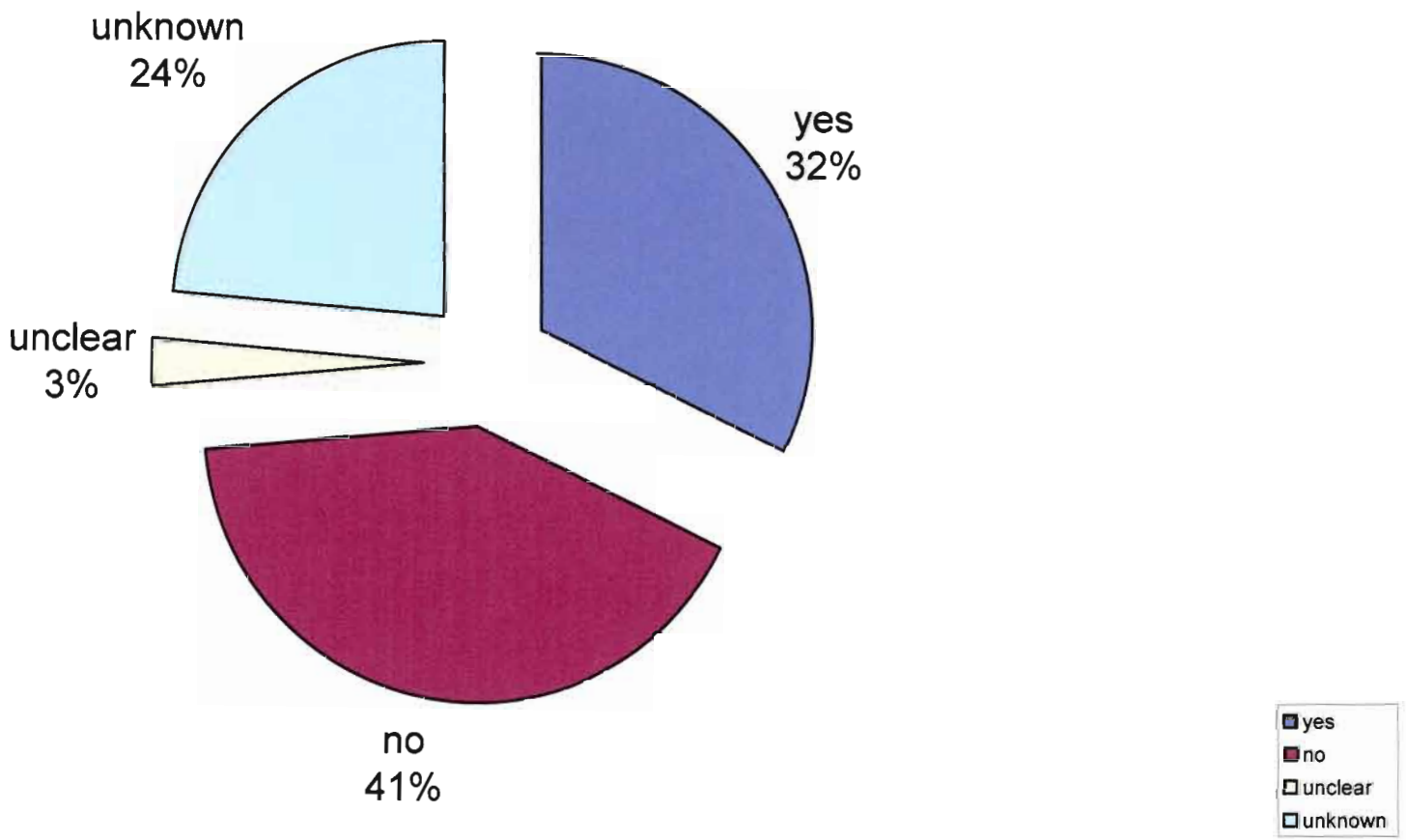
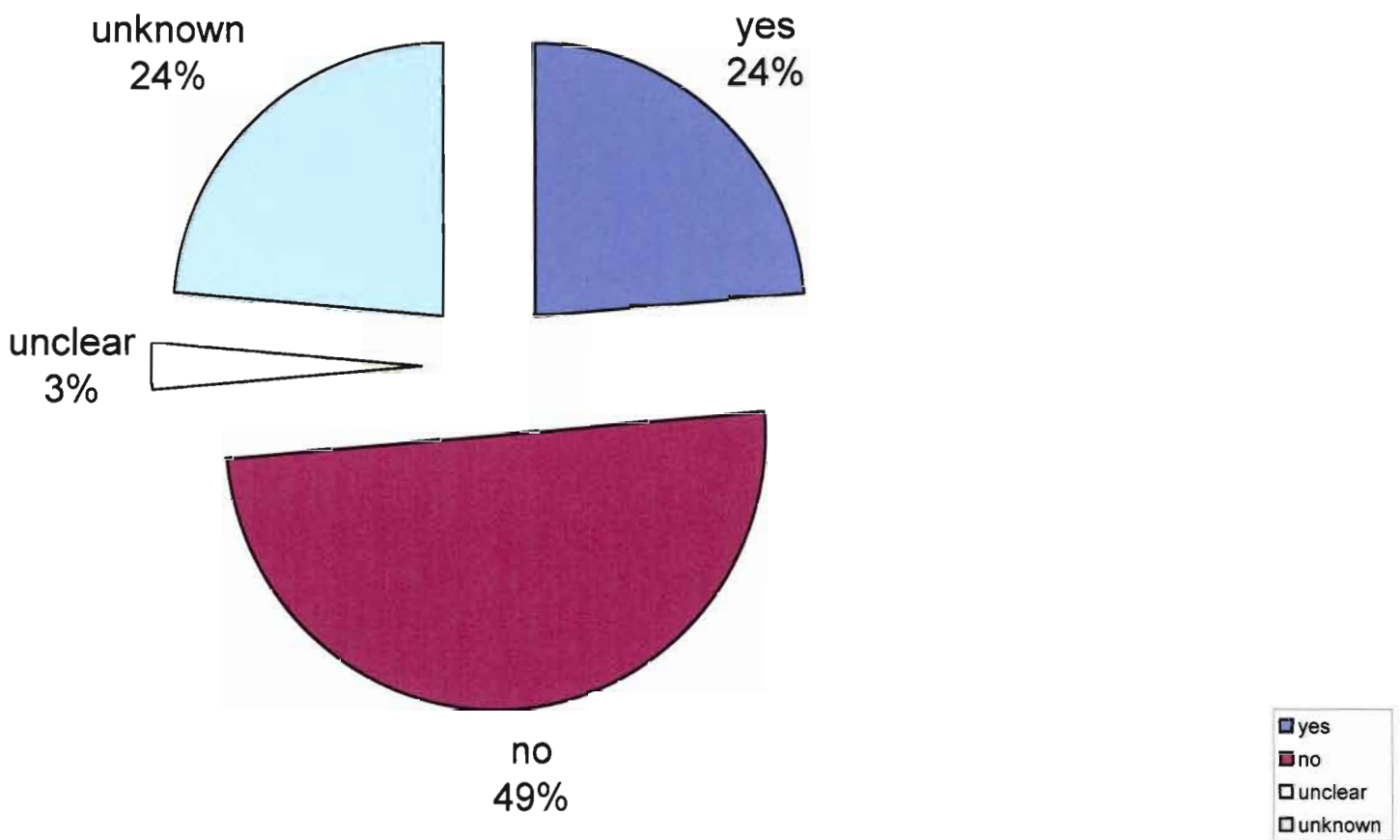
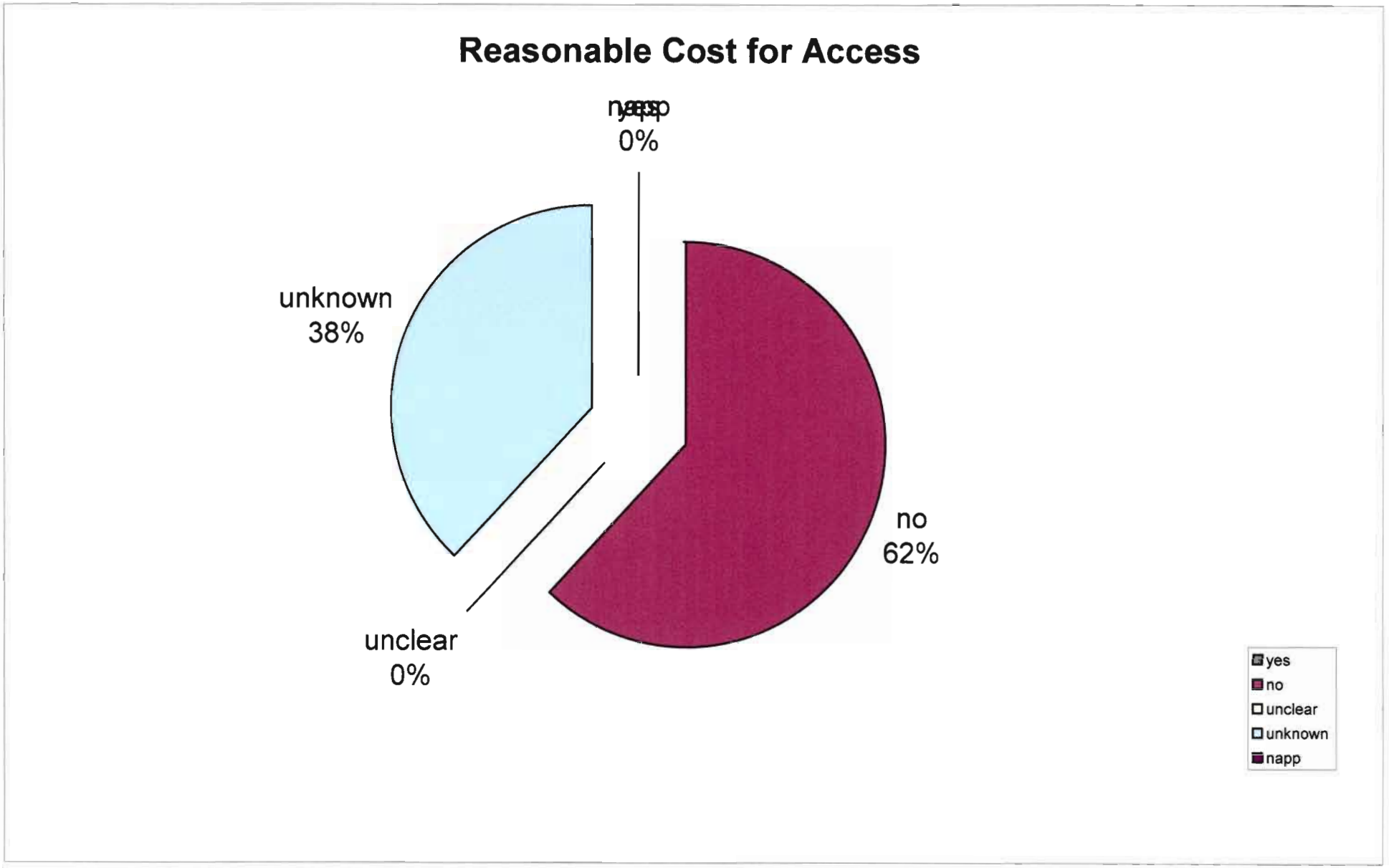


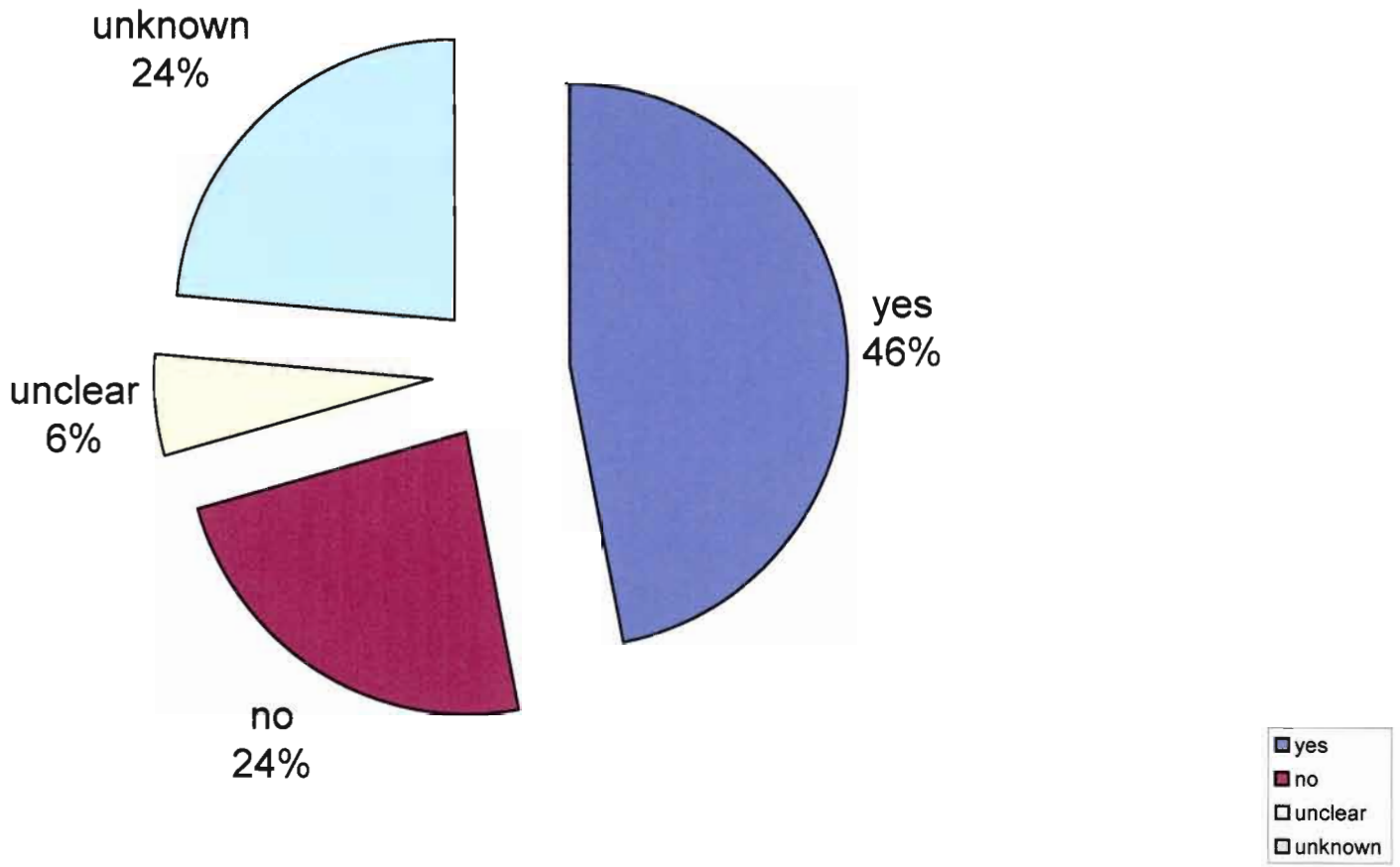
Table 2.5

Reasonable Access Provided




Reasonable Cost for Access
napp
0%
unknown
38%
no
62%
unclear
0%
yes
no
unclear
unknown
napp

Correction/Amendment of inaccurate data



Deletion of inaccurate data

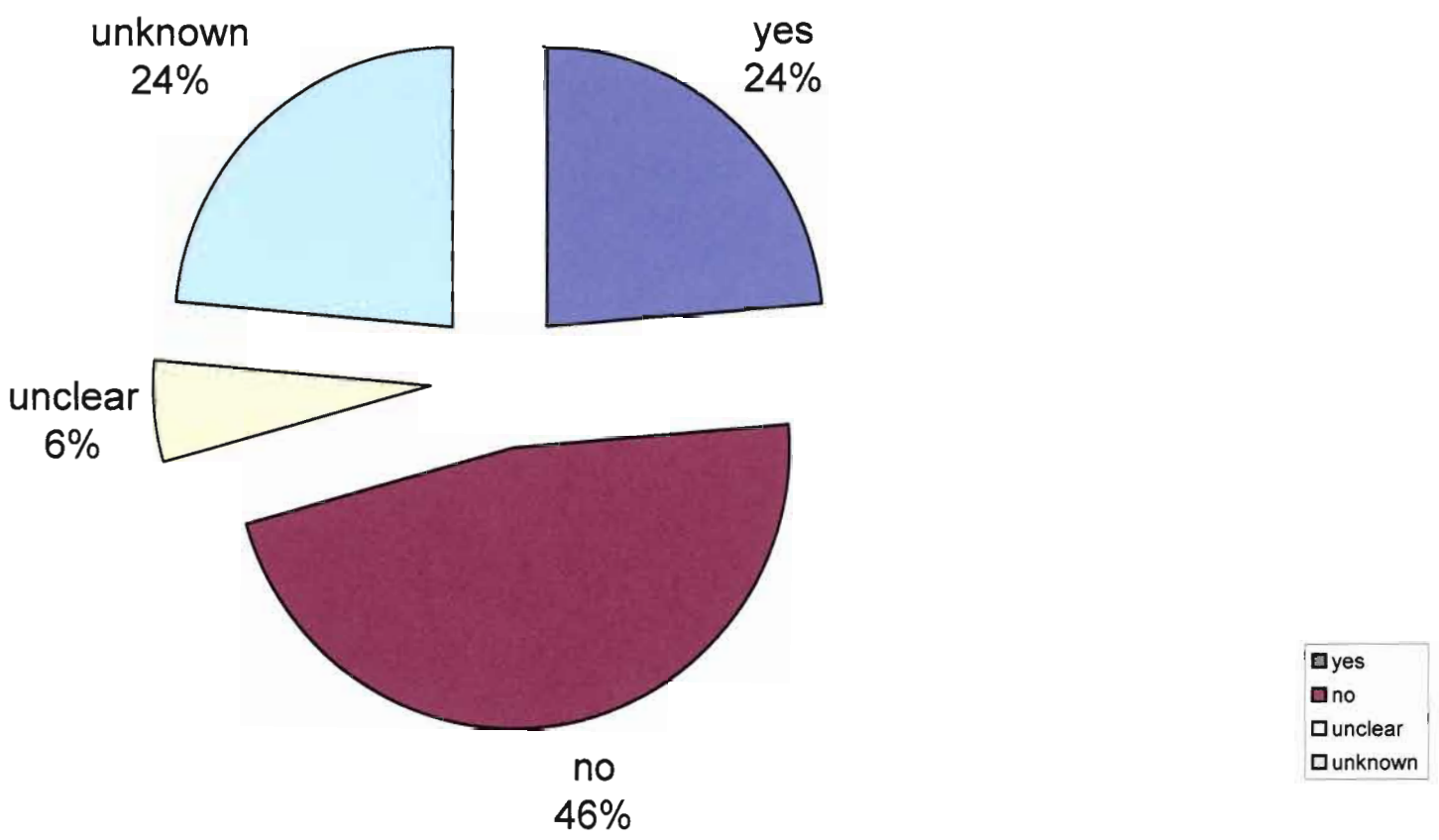
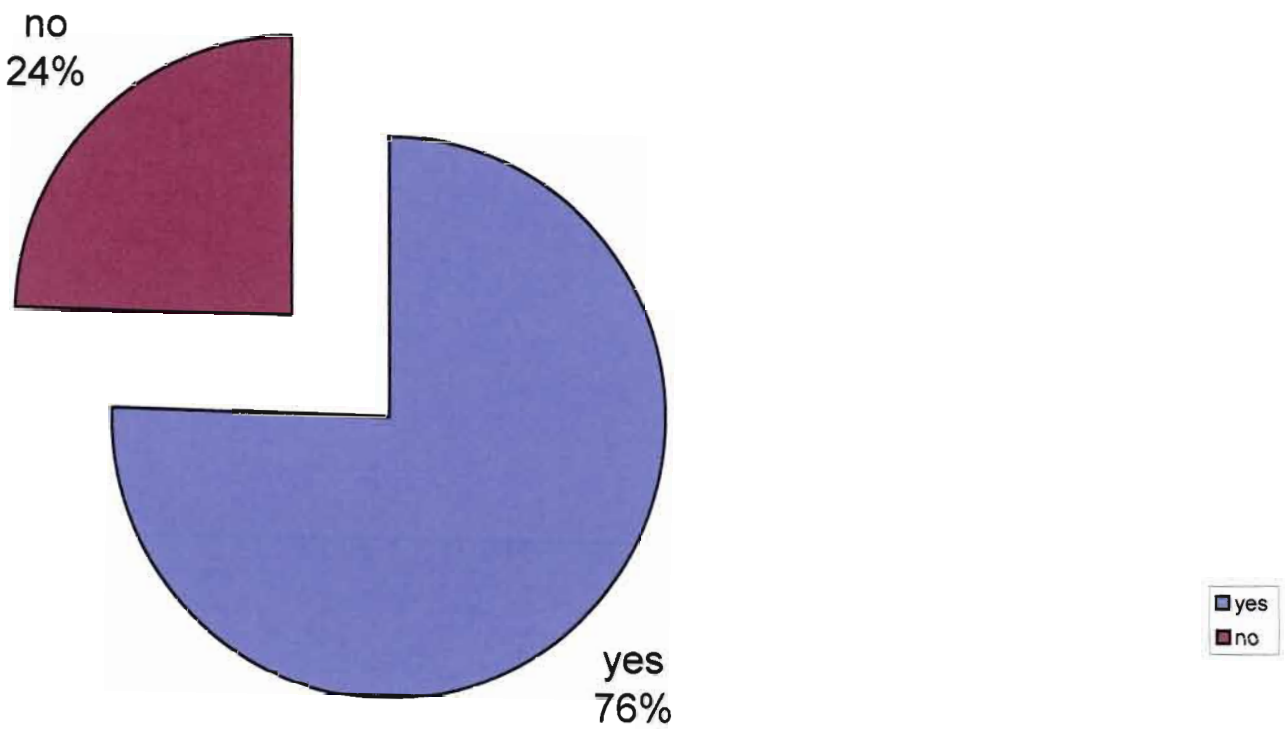
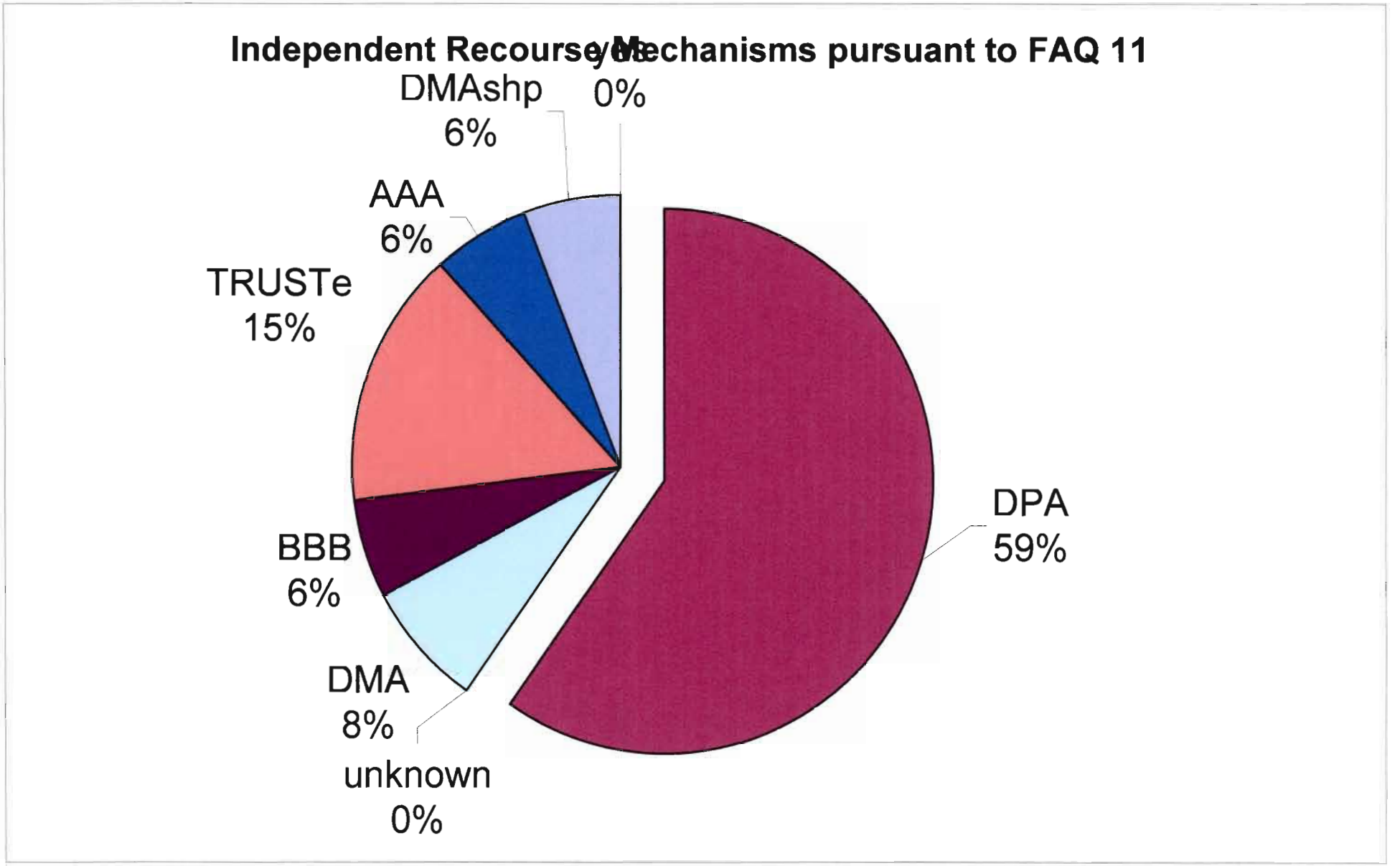


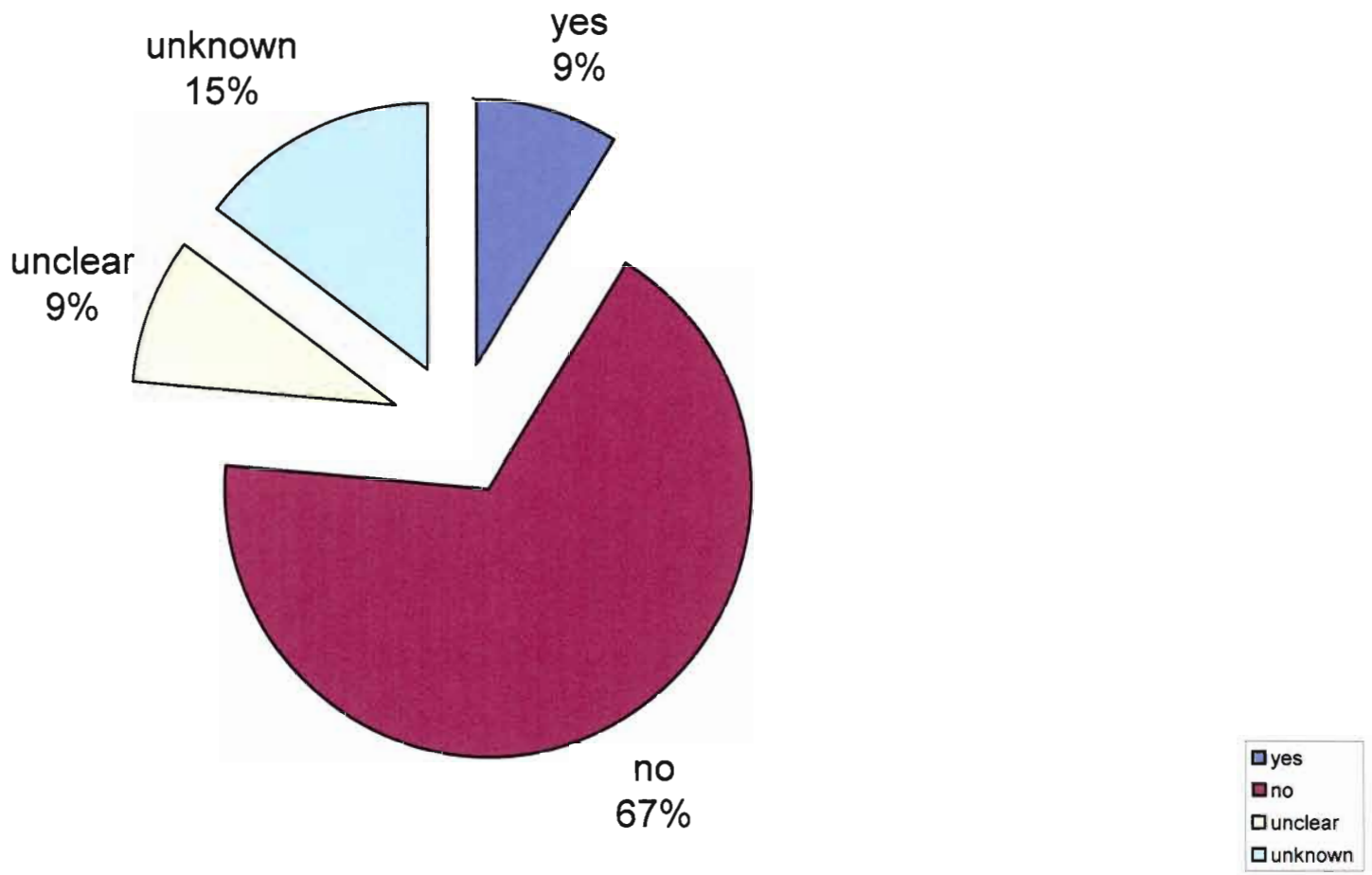
Table 3.1

Independent Recourse Mechanisms pursuant to FAQ 5




Independent Recourse Mechanisms pursuant to FAQ 11
DMAshp
6%
0%
AAA
6%
TRUSTe
15%
DPA
59%
BBB
6%
DMA
8%
unknown
0%

Obligation to Remedy problem



Sanctions for Violations

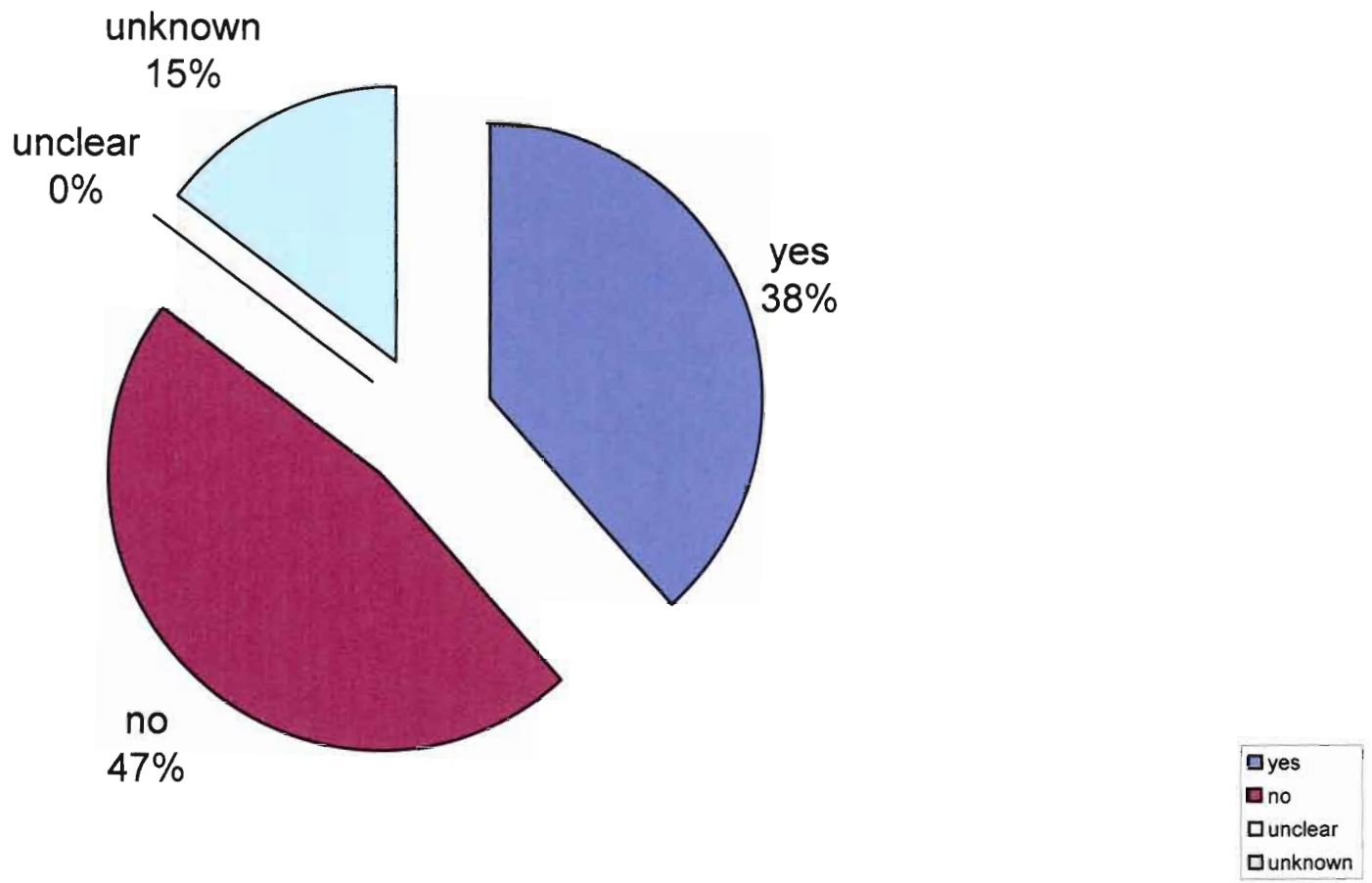
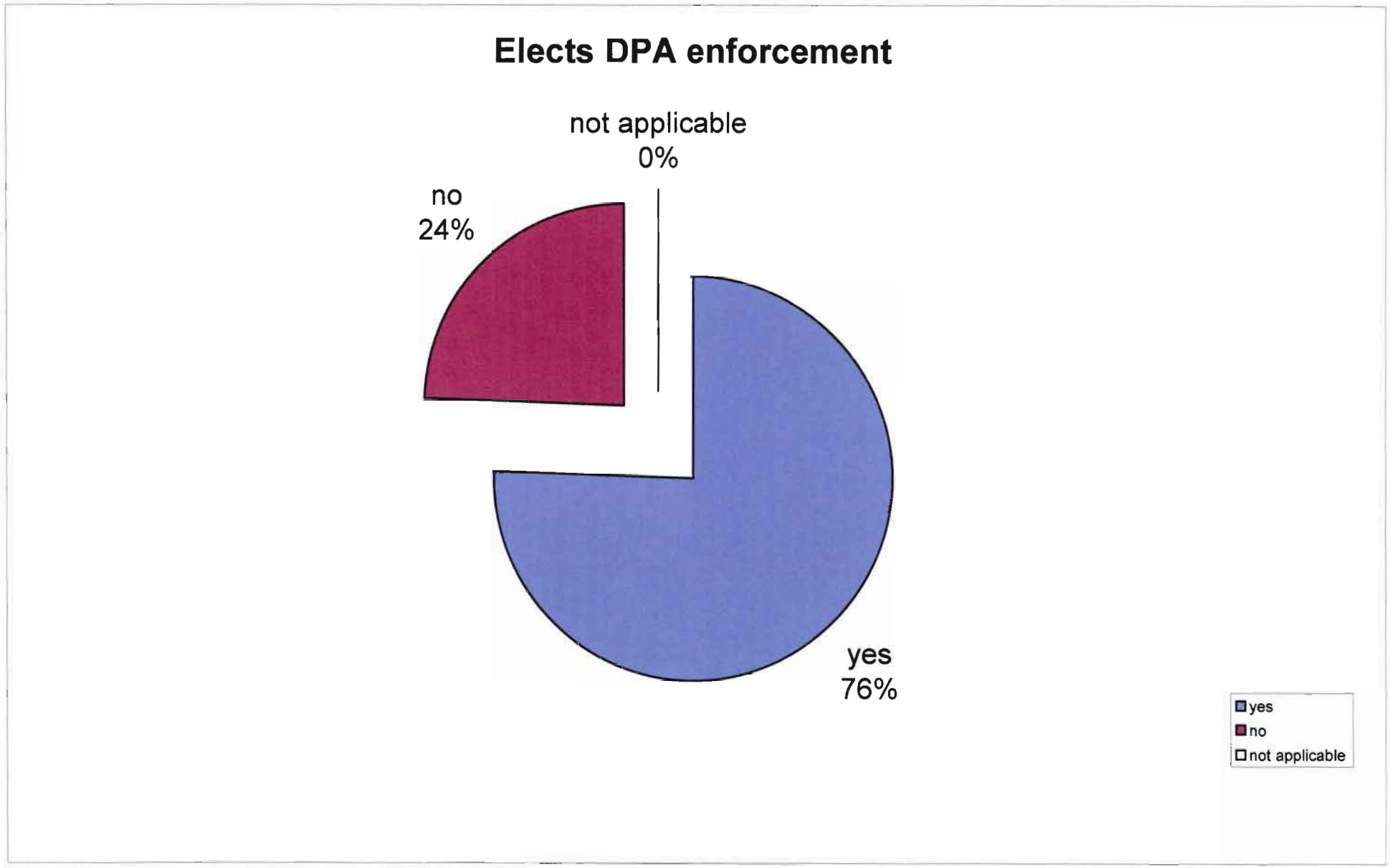
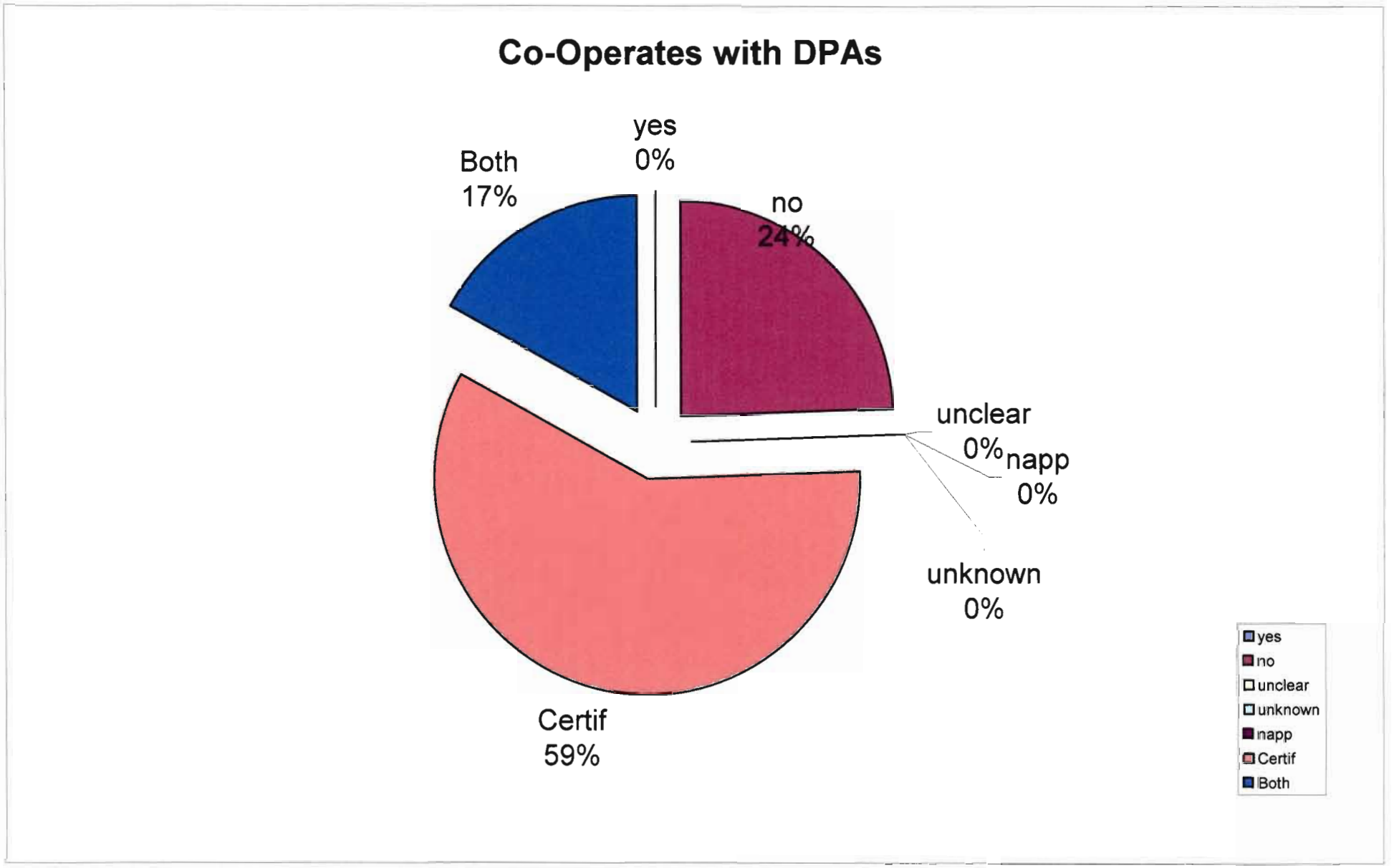


Table 3.2


Elects DPA enforcement
not applicable
0%
no
24%
yes
76%
yes
no
not applicable


Co-Operates with DPAs
yes
0%
Both
17%
no
24%
unclear
0%
napp
0%
unknown
0%
Certif
59%
yes
no
unclear
unknown
napp
Certif
Both

Agrees to comply with DPA advice

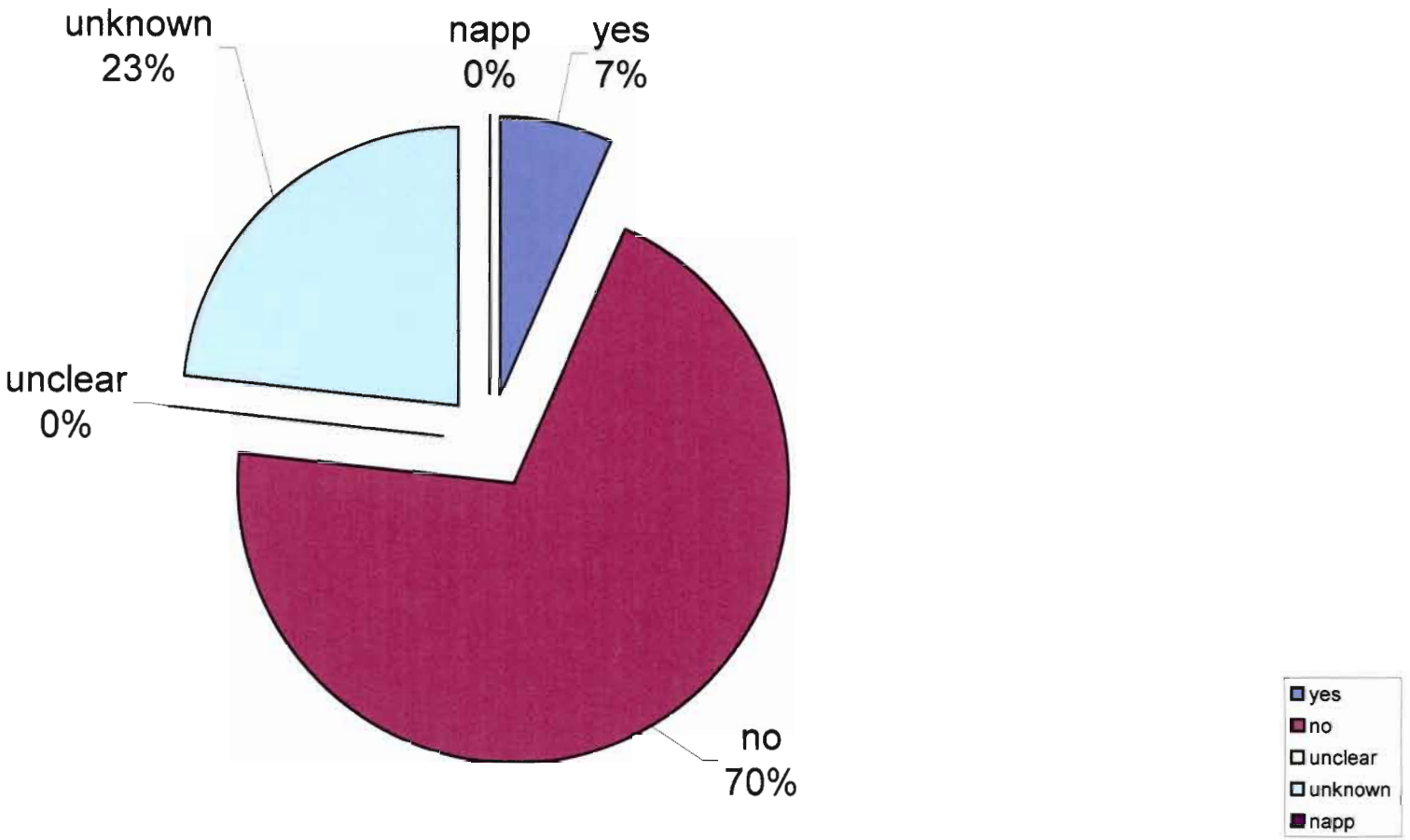
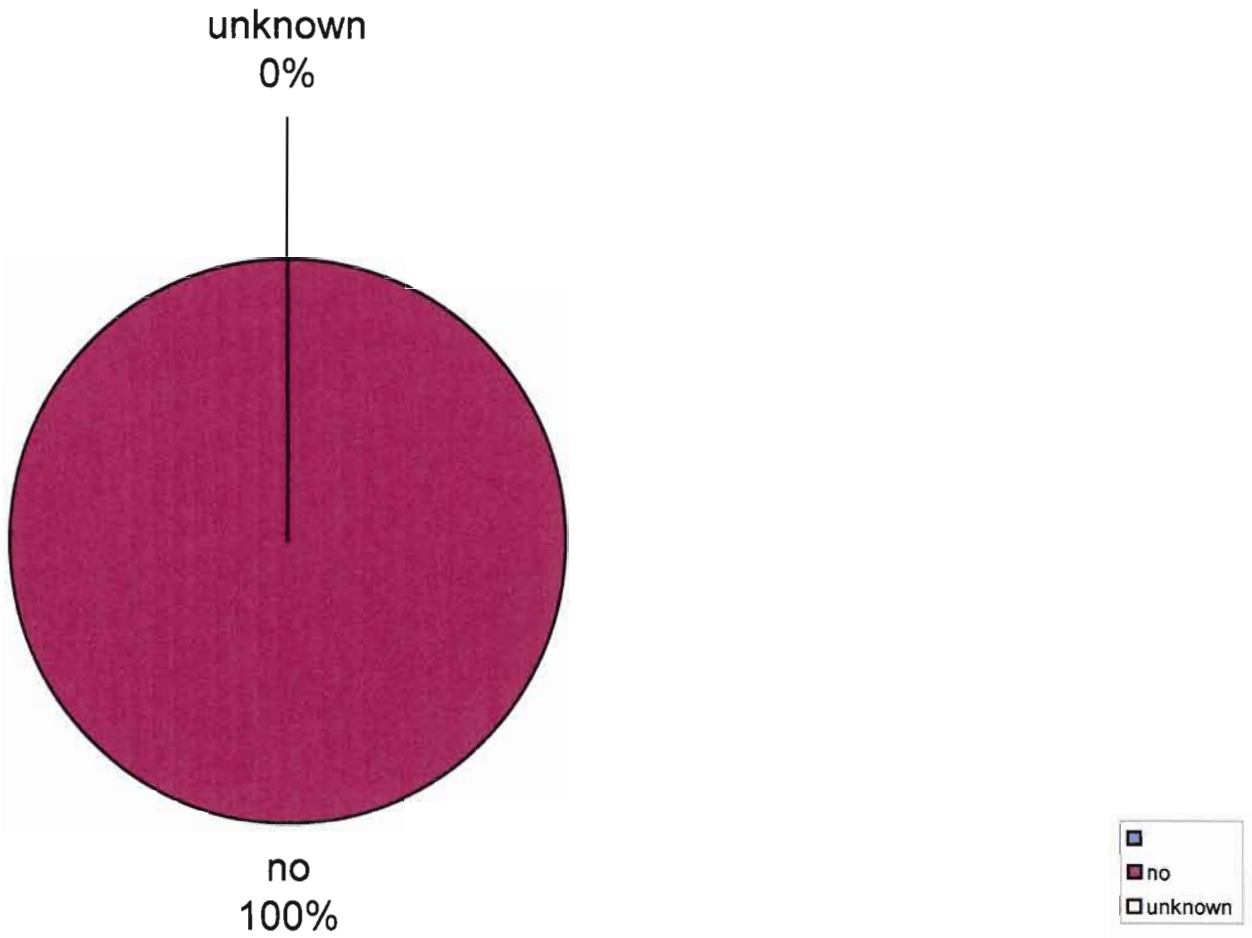
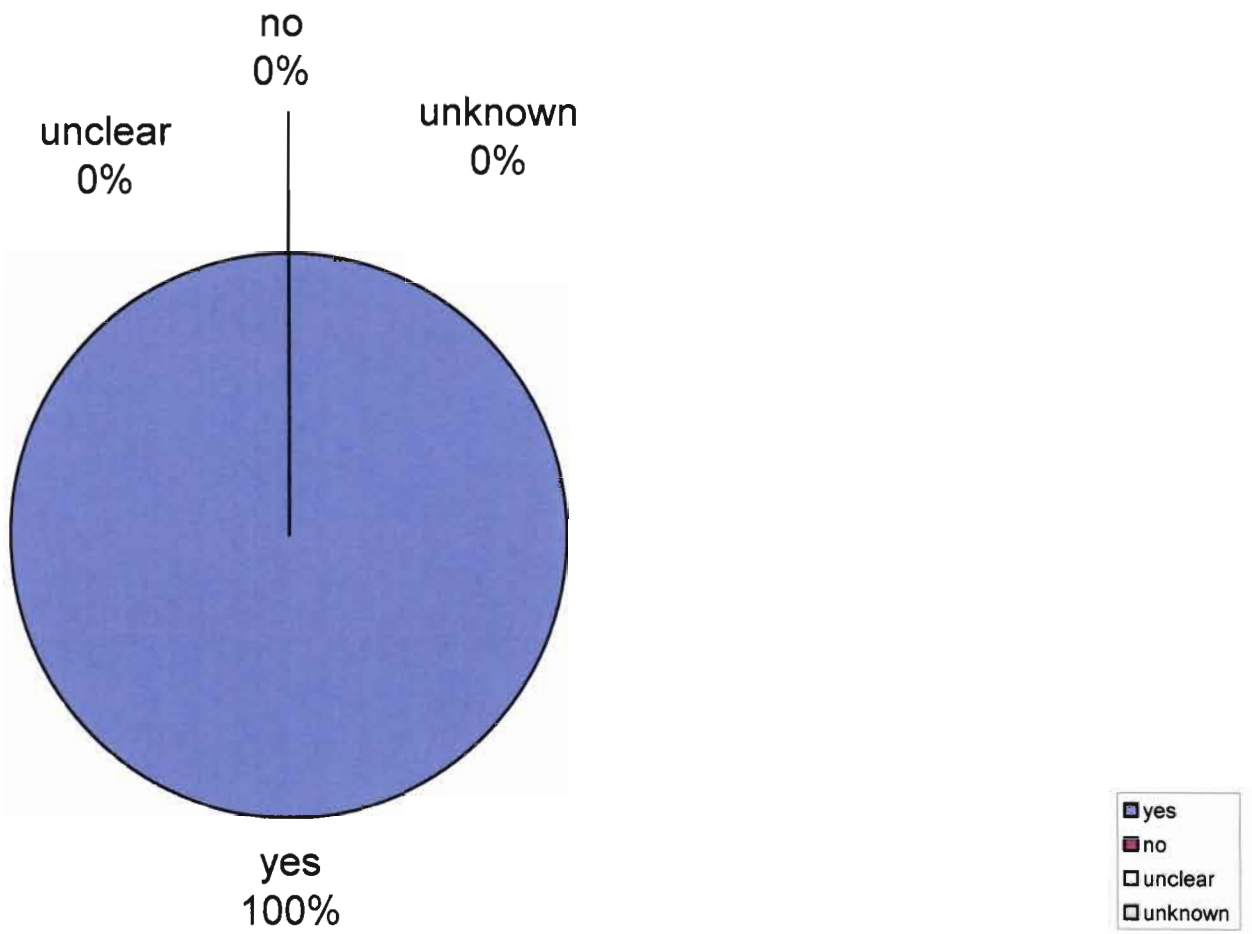


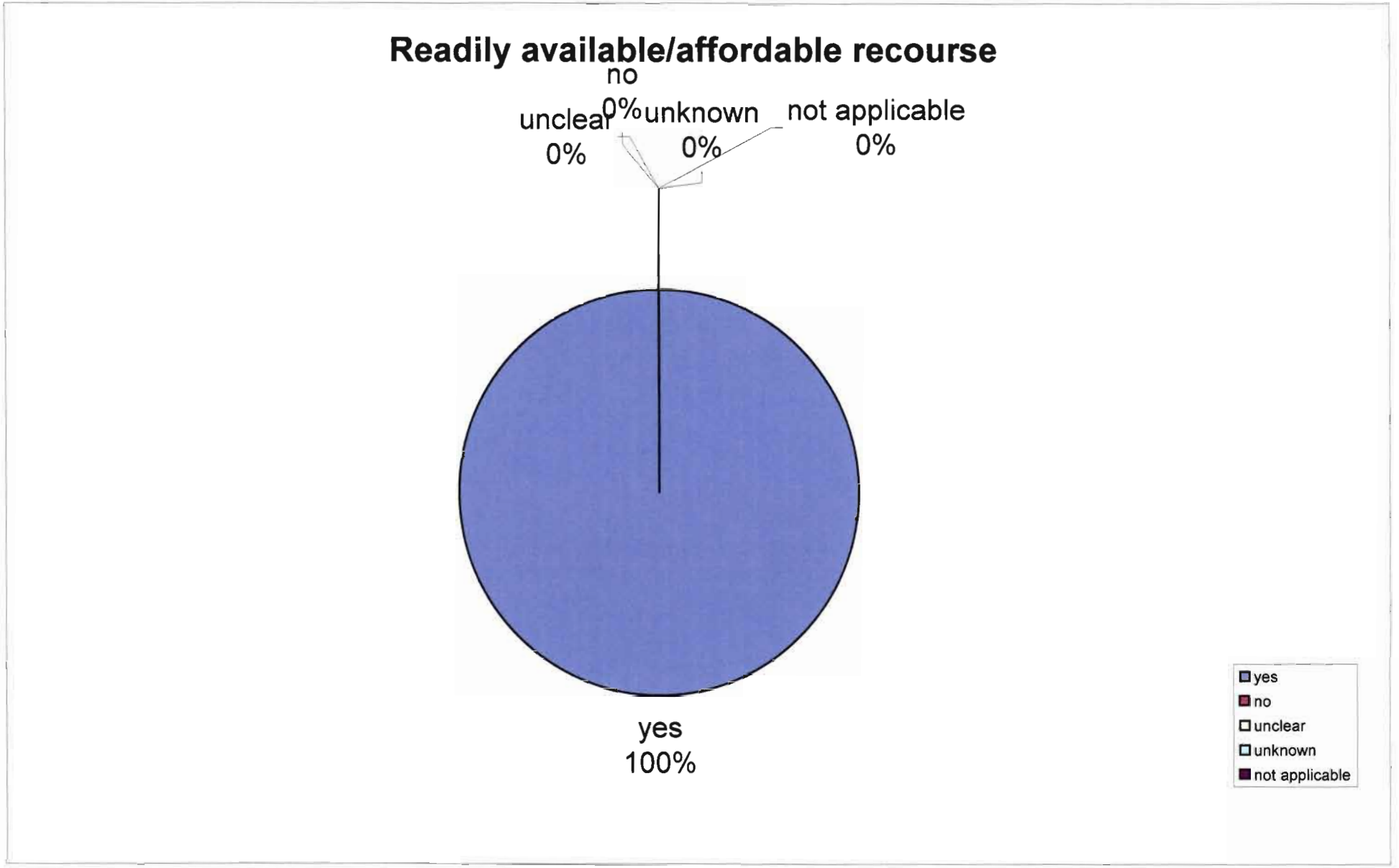
Table 3.3

US Legal or Regulatory Supervision

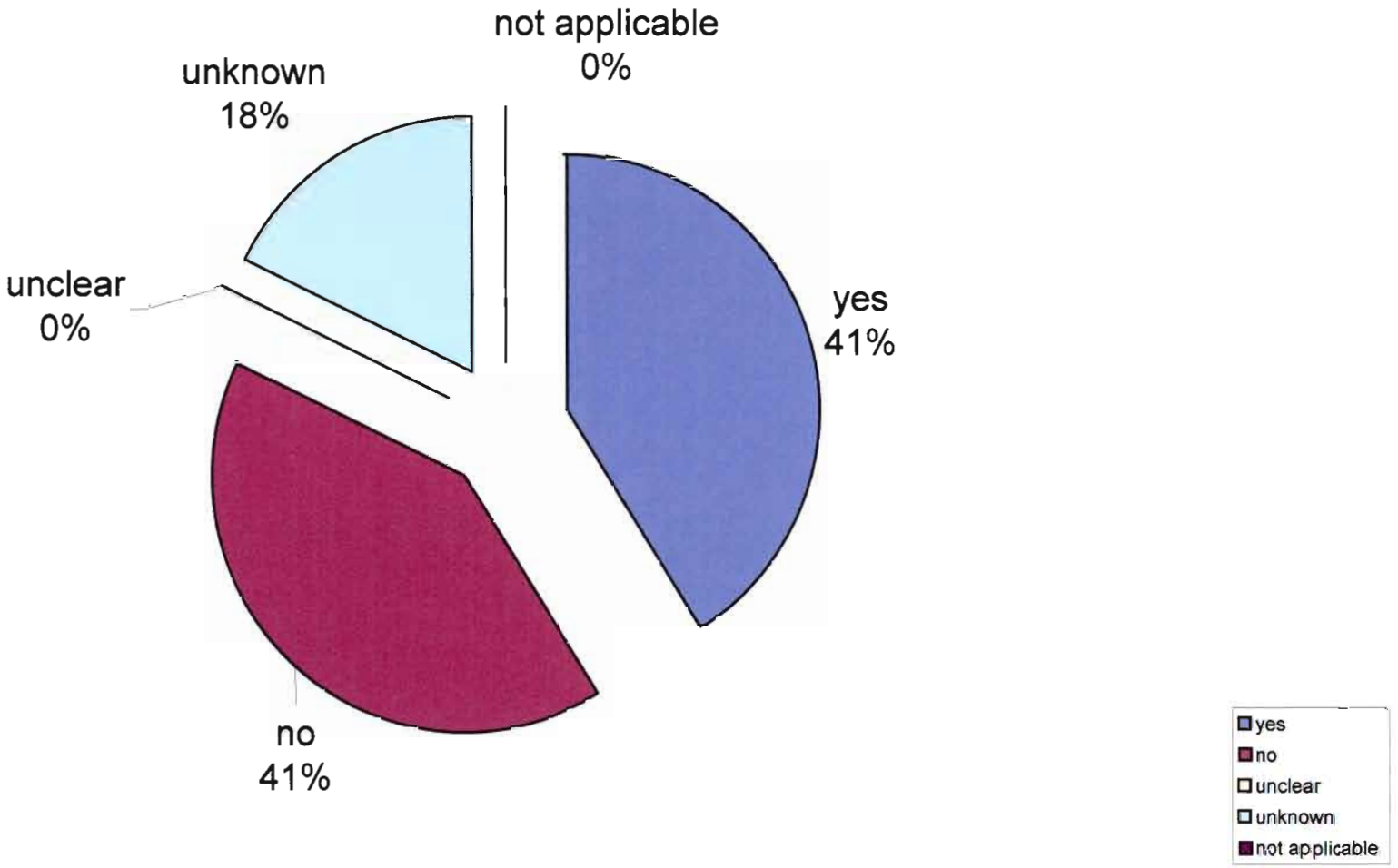


Independence of Recourse Mechanism

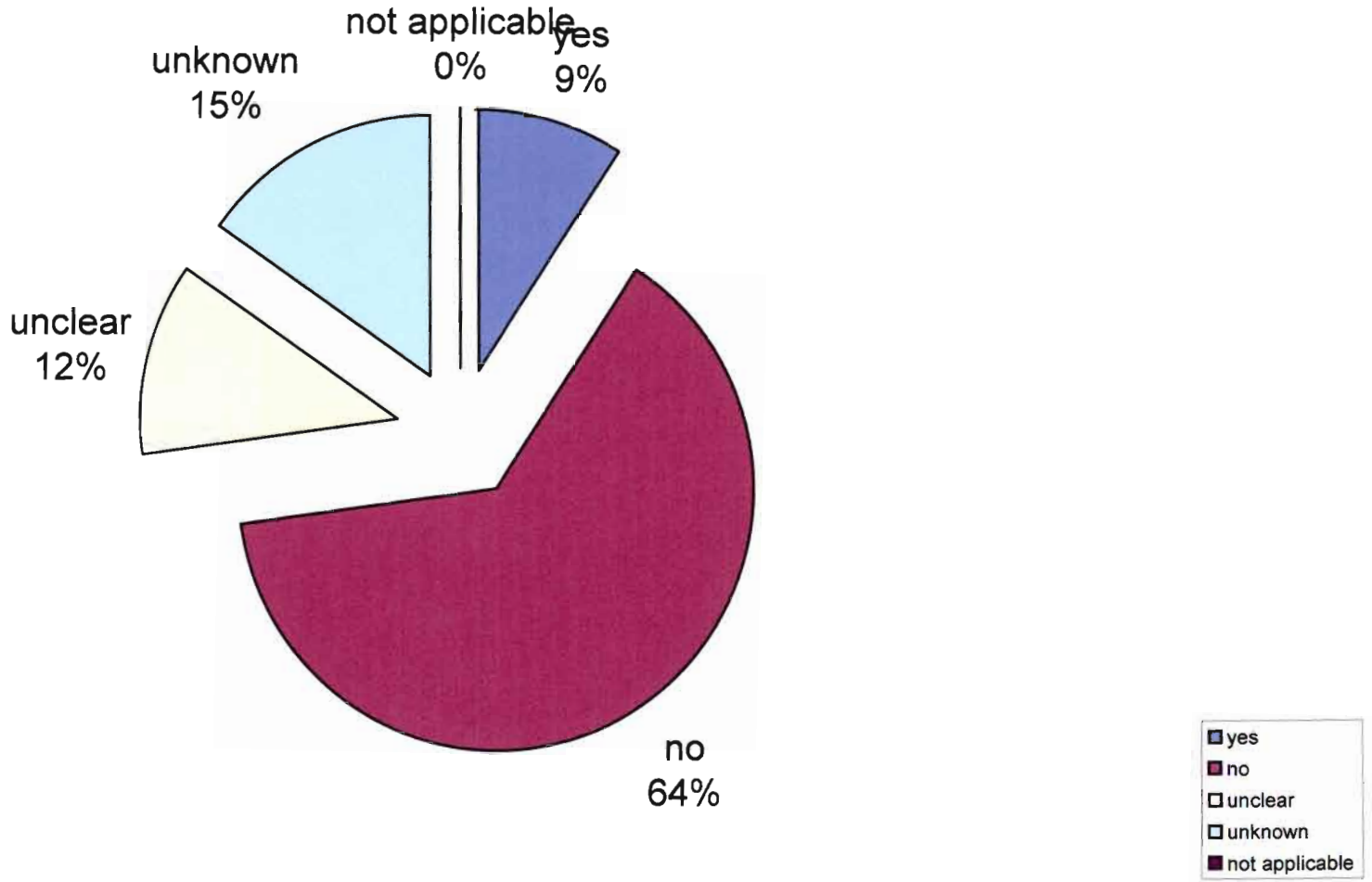



Readily available/affordable recourse
no
0%
unclear
0%
unknown
0%
not applicable
0%
yes
100%
yes
no
unclear
unknown
not applicable

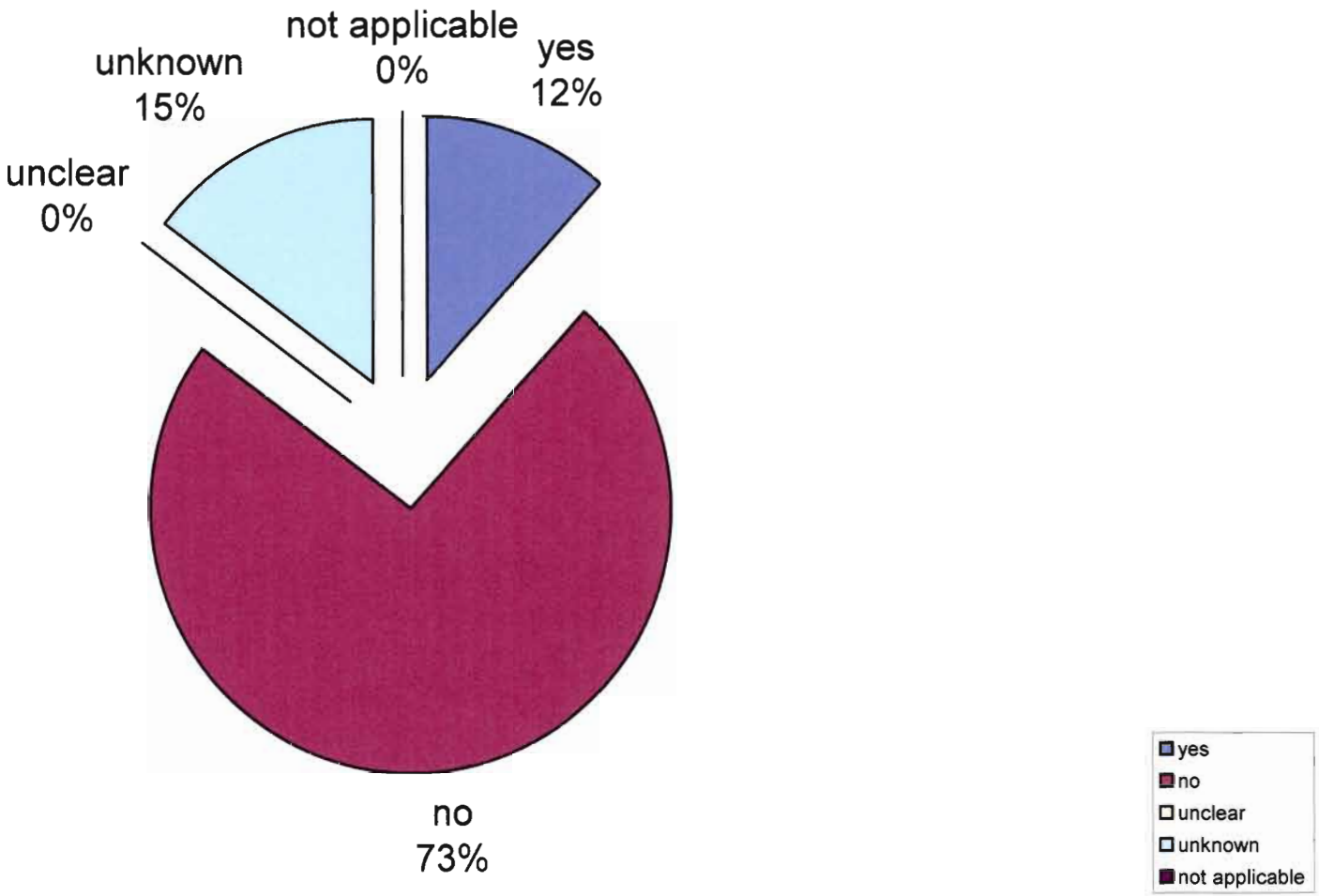
Transparency of Dispute Resolution Procedures



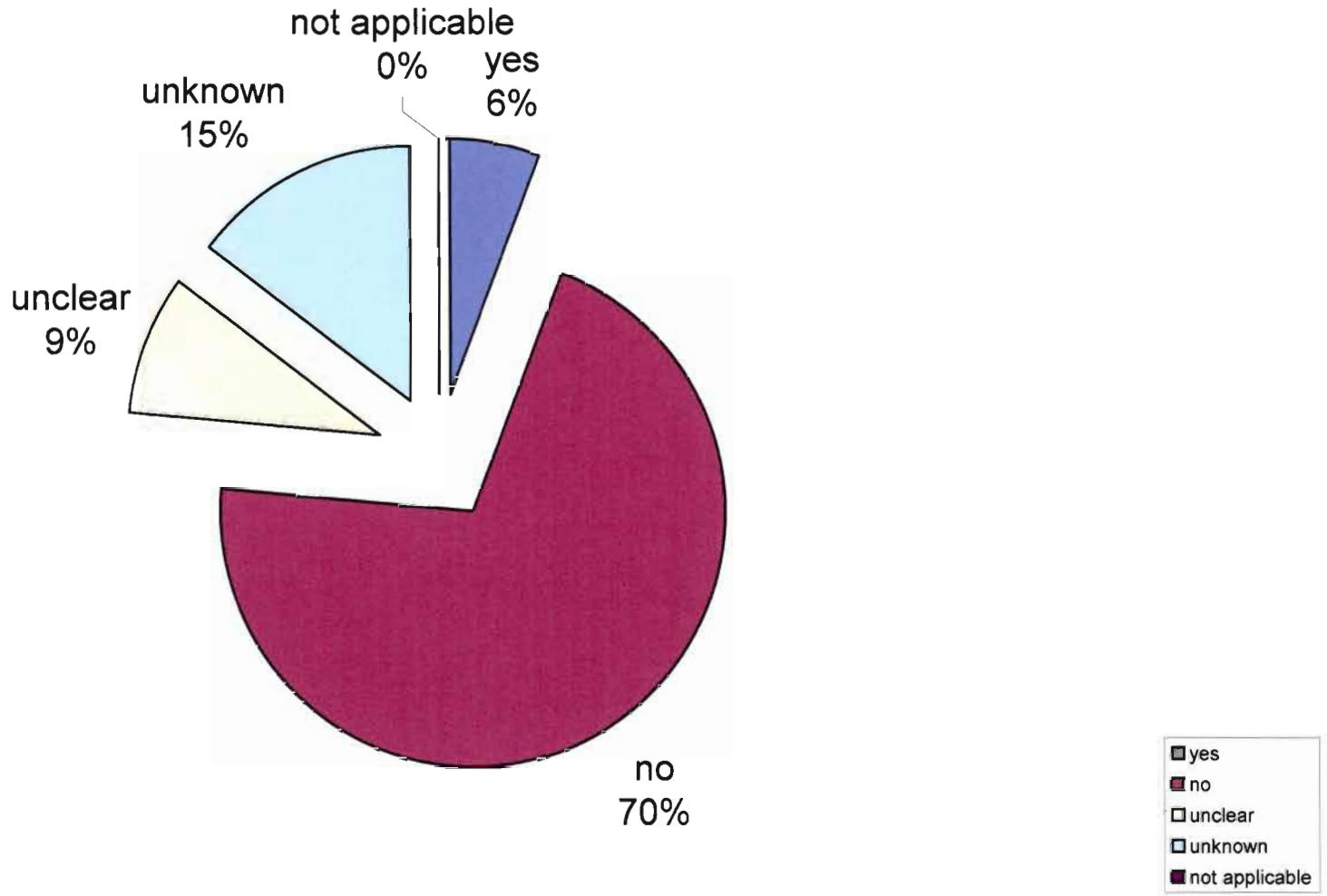
Company agrees to reverse effects of breach

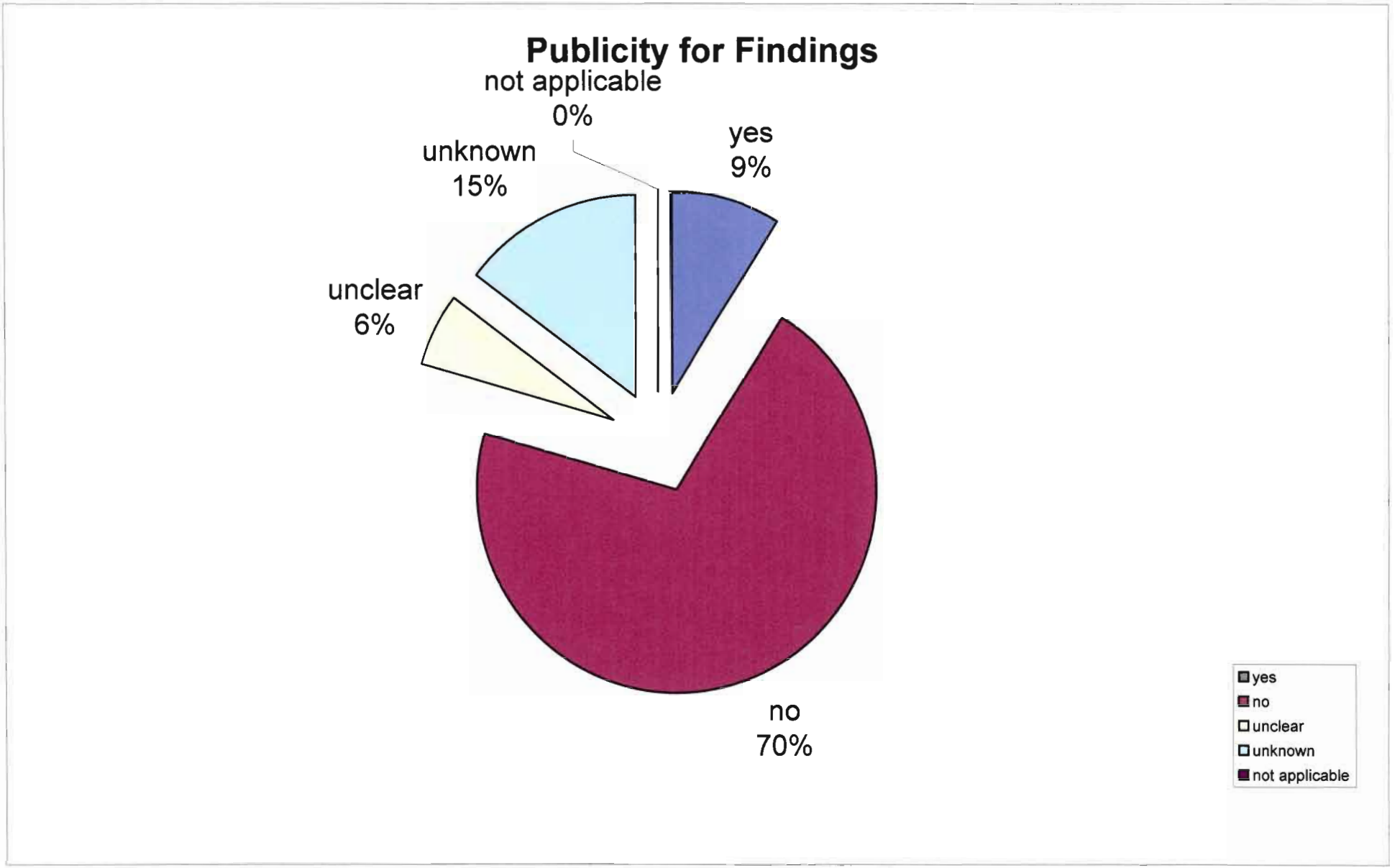


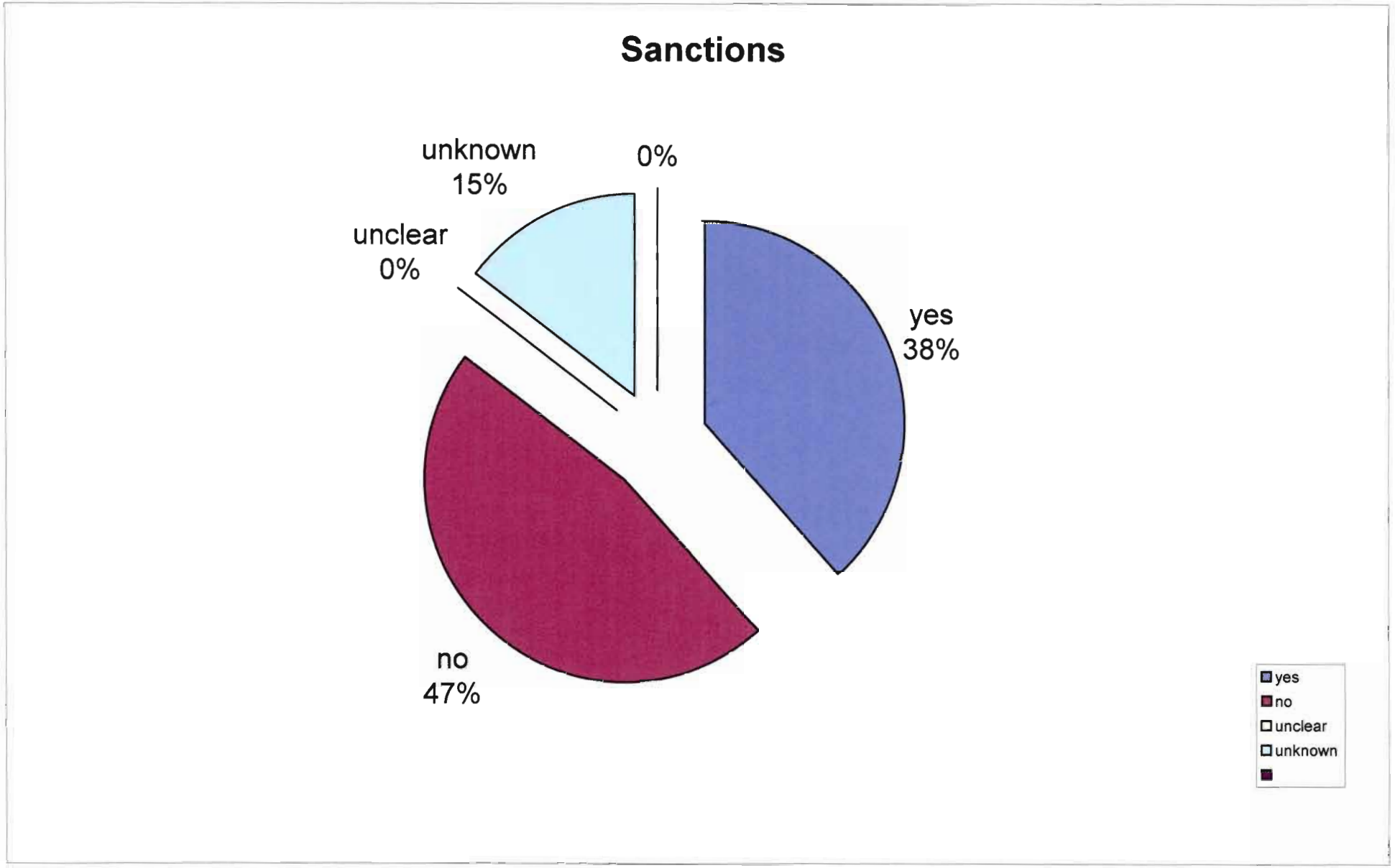
SH Compliant Future Processing



Cessation of Processing of Data for Harmed Individual




Publicity for Findings
not applicable
0%
yes
9%
unknown
15%
unclear
6%
no
70%
yes
no
unclear
unknown
not applicable


Sanctions
unknown
15%
0%
unclear
0%
yes
38%
no
47%
yes
no
unclear
unknown

APPENDIX VII

Data Protection Authorities answers to the questionnaire of point 2.4.b)

	Notification of data transfers	Number of data transfers under SHA	Type of data transfers and amount	Intra/Extra company transfers	Different treatment if cooperation with DPA	Publication of guidelines/opinions for SHA use	Complaints: amount, nature, treatment, investigation, coordination with FTC	Communication from FTC to investigate	Approach to FTC	Suspention of data flows (Art. 3 SHA)	Information procedure (Art. 3.1.a))	Limitation of SHA due to national security, public interest, etc.	Number of people within the DPA working on TBDF	Further information added
Austria														
Belgium	yes	18 transfers have been declared under SHA until September 2001, among which 8 notifications between January and December 2003	14 HR; 1 identification data; 1 consumer data; 2 inside training data	all intra-company	no	on TBDF in general (ADD LINK)	no complaint	no	no	no	no	no	2 lawyers and 1 member are experts in the issue	from their experience: it seems that the SHA and the standard contractual clauses are not broadly used yet. SHA is mentioned in less than 10% of TBDF notified. The main legal basis for TBDF is consent and the fact that the TBDF is necessary for the performance of a contract. In more than half of the cases, several legal basis are used in order to secure the validity of a TBDF.
Denmark	no	napp	napp	napp	napp	ADD LINK	no complaint	no	no	no	no	no	1	
Finland	no if TBDF based on SHA	napp	napp	napp	no experience	on TBDF in general (ADD LINK)	no complaint	no	no	no	no	no	1 plus Data Protection Ombudsman himself	
France														
Germany	no	napp	napp	napp	no experience	no	no complaint	no	no	no	no experience	no	1	German companies tend to use the EU model clause or BDR for TBDF to the US rather than rely on the quite complex (and in respect of the categories of data non-concluding) SHA
Greece														
Iceland														

Ireland	no	napp	napp	napp	no experience	no. Presentations to data controllers and companies including specific advice and guidance	no complaint	no	no	no	no	no	none exclusively. All the staff deal with telephone enquiries.	
Italy	Prior to 1-01-04 all TBDF has to be notified. After that date notification of only certain categories of personal data.	Results of a survey	Results of a survey	Results of a survey (mainly intra-company and in particular related to HR	no difference is made in this regard	No specific guidelines	no complaint	no	no	no	no	no	7	Reference may be made to some cases addressed by the Italian Garante, in which US-based companies appeared to prefer to avail themselves of standard contractual clauses (SCC) for transferring data to the US because they found that the SCC were more in line with EU data protection principles compared with the SHA. Additionally, the standard contractual clauses were considered to provide more clear-cut guidelines as to liability issues and implementing mechanisms.
Linchtenstein														
Luxemburg	notification a posteriori, but the law does not explicitly mention the need of indication of the legal basis (art. 19.2)				no experience	recomendation of use of other DPAs documents and EC and Art. 29 WP documents	no under SHA	no	no	no	no	no	3 permanent and 3 substitute members compose the DPA. 6 to 8 employees able to work on TBDF too.	no
Norway														
Portugal	yes (art. 27 Law 67/98). The DPA issues a permit, allowing the flow and stating any necessary or additional conditions.	napp	outside the SHA, the great majority of TBDF to the US concerns HR data.	napp	napp	no. Just a link to the FTC.	no complaint	no	no	no	no	no	10	It is curious that controllers do not use SHA as a legal ground for TBDF to US, which would be easier to get a permit, but instead recourse to other instruments. We may say that SHA is far from being a successful solution in Portugal to TBDF to US.

Spain	yes+B3	16	10 on HR, 6 customers data	intra	no	The SDPA issued Instruction 1/2000 of 1 December 2000 on the rules governing international data transfers with guidelines covering all cases of international data flows including Safe Harbor	no complaint	no	no	no	SDPA has not been informed of any decision taken by the Federal Trade Commission, the US Department of Transportation or any of	question was thoroughly discussed and strongly opposed by the Article 29 Working Party during the Safe Harbor negotiations. The SDPA agrees	3	1) In general, it must be mentioned that companies established in Spain rather like other systems (mainly the use of contractual clauses or asking for the consent of data subjects) than the Safe Harbor approach for legitimating the transfers of personal data to the US. This is even more true since the approval by the European Commission of the Model Contractual Clauses. The most used argument in favour of this approach is the legal certainty provided by the other methods is greater than the ambiguous, complex and less than clear provisions of the Safe Harbor Agreement.
Sweeden	no	napp	napp	napp	napp	no	no complaint	no	no	no	no	no		
The Netherlands	"yes" if the processing activity has to be notified, "no" if processing itself is exempted	napp	napp	napp	napp	LINK	no complaint	no	no	no	no	no	2 staff members work on a regular basis (half time) on TBDF, 34 other membrs work occasionally.	

UK	no. Controllers are required to specify TBDF, but not the country of destination	napp	napp	napp	napp	document on website ADD LINK	no. If any complaint be received it would be dealt with in the same manner as anny other complain to the office (Section 42 of the Data Protection Act 1998)	no	no	no	no (SEE NOTE BELOW)	no	4	The fact that no complaints have arisen regarding the SHA appears to indicate that they are working well. Recognition of importance of TBDF restrictions to avoid circumvention of EU law.If eveidence of breach action would be taken.

APPENDIX VIII

Comparative Analysis of SH, Model Contractual Clauses and Binding Corporate Rules

	SHA	Standard Contractual Clauses Decision (controller to controller)	Article 29 Working Party Working Document on Binding Corporate Rules (no EC Decision adopted yet)
Material Scope	Material limitation: determined by jurisdiction of FTC and DoT, personal data as defined in the Directive	personal data as defined in the Directiveno limitation	Personal data as defined in the Directive no limitation
Personal Scope	US Organizations, data controllers and data processors	Third Country Data controllers	Corporations
Territorial Scope	TBDF to the US	TBDF from EU to any country not providing adequate protection	TBDF among corporate members established either in countries providing adequete protection or not
Legal basis	Art. 25(6) Dir. 95/46	Art. 26(2) Dir. 95/46	Art. 26(2) Dir. 95/46
Binding nature	yes upon adherence	yes upon signature	(potentially) yes upon adoption
Purpose limitation	integrity principle	yes: clause 2; Appendix 2 & 3	point 4.1
Data quality and proportionality	Data integrity pple	Appendix 2 & 3	point 4.1
Transparency	Notice and choice pple	Appendix 2	point 4.1
Security	Security pple	Appendix 2	point 4.1
Access, rectif., oposit.	Access pple	Appendix 2 & 3	point 4.1
Onward transfers	Onward transfer pple	Appendix 2 & 3	point 3.2, point 4.1
Sensitive data	Choice pple (opt-in)	Appendix 2	point 4.1
Good level of compliance			point 4.1, 5.1, 5.2, 5.3
Support and help to individual data subjects			point 4.1, 5.3, 5.4
Appropriate redress	enforcement principle	several liability and accept advice of the DPA	point 4.1
3rd party beneficiary clause	no (the SH is not a contract but a declaration of adequacy)	yes	yes, point 3.3.2

Joint & several liability	no	yes	no, the European member with delegated data protection responsibilitis should accept responsibility for, and agree to take the necessary action to remedy the acts of other members of the corporate group outside the Community, and where appropriate, pay compensation. Inversion of the brden of proof. point 5.5.2
Cooperation with DPAs	optional; mandatory if human resources processed	yes	yes
Obligation to comply with DPA advise	yes if chosen as dispute resolution mechanism and if human resources data processed	is this lacking?	
Audits	no	at request of the data exporter	point 5.2
Governing law	US	Law of the Member State where the exporter is established	free to determine
Jurisdiction	FAQ 11 (privacy program including enforcement mecanism -ADR-, compliance with legal or regulatory authorities, commitment to cooperate with DPA)	Data subject decides whether refer the dispute to: mediation by an independent person or by the supervisory authority; the courts in the Member State where the exporter is established. The parties may agree to refer the dispute to an arbitration body.	competent DPA or competent court on Community territory, point 5.6